Python 872 Install Manual

MySQL Reference ManualDeep Learning for Computer VisioniOS Hacker's HandbookProgramming PythonA Primer on Scientific Programming with PythonPenetration TestingThe Art of Network Penetration TestingThe Practice of System and Network AdministrationLearning Kali LinuxHow Linux Works, 2nd EditionLearn Ethical Hacking from ScratchLearning Malware AnalysisProgramming: 4 Manuscripts in 1 Book: Python for Beginners, Python 3 Guide, Learn Java, Excel 2016System Programmer's Guide to Z/OS System LoggerPython for Data AnalysisThe Zope BookWindows 10 Inside Out (includes Current Book Service)Complete A+ Guide to IT Hardware and SoftwarePython for Data AnalysisWireshark for Security ProfessionalsWindows 7 Inside OutMicrotimesThe Hacker's KeyBeginning Game Development with Python and PygameUsing Mathematica for Quantum MechanicsPython for BioinformaticsSiren StatusIBM Spectrum Protect Plus Practical Guidance for Deployment, Configuration, and UsageNetwork Scanning CookbookLinux Basics for HackersIBM AIX Enhancements and ModernizationBeagleBone: Creative Projects for HobbyistsHacking and Penetration Testing with Low Power DevicesFinancial Risk Modelling and Portfolio Optimization with RDiscrete Choice Methods with SimulationA Practical Guide to Ubuntu LinuxPython and HDF5Unix Power ToolsNumerical Methods in Engineering with PythonRed Hat RHCSA/RHCE 7 Cert Guide

MySQL Reference Manual

IBM® Spectrum Protect Plus is a data protection solution that provides near-instant recovery, replication, retention management, and reuse for virtual machines, databases, and applications backups in hybrid multicloud environments. IBM Knowledge Center for IBM Spectrum® Protect Plus provides extensive documentation for installation, deployment, and usage. In addition, build and size an IBM Spectrum Protect Plus solution. The goal of this IBM Redpaper® publication is to summarize and complement the available information by providing useful hints and tips that are based on the authors' practical experience in installing and supporting IBM Spectrum Protect Plus in customer environments. Over time, our aim is to compile a set of best practices that cover all aspects of the product, from planning and installation to tuning, maintenance, and troubleshooting.

Deep Learning for Computer Vision

This comprehensive reference guide offers useful pointers for advanced use of SQL and describes the bugs and workarounds involved in compiling MySQL for every system.

iOS Hacker's Handbook

Presents case studies and instructions on how to solve data analysis problems using Python.

Programming Python

This book Includes 4 Manuscripts in 1 book: - Python For Beginners: A Crash Course Guide To Learn Python in 1 Week - Python 3 Guide: A Beginner Crash Course Guide to Learn Python 3 in 1 Week - Learn Java: A Crash Course Guide to Learn Java in 1 Week - Excel 2016: A Comprehensive Beginner's Guide to Microsoft Excel 2016 Python For Beginners: A Crash Course Guide To Learn Python in 1 Week Here what you'll learn after downloading this Python for Beginners book: ✓Introduction ✓Chapter 1: Python: A Comprehensive Background ✓Chapter 2: How to Download and Install Python ✓Chapter 3: Python Glossary ✓Chapter 4: Interacting with Python ✓Chapter 5: Using Turtle for a Simple Drawing ✓Chapter 6: Variables ✓Chapter 7: Loops ✓Chapter 8: Native Python Datatypes ✓Chapter 9: Python Dictionaries ✓Chapter 10: Boolean Logic and Conditional Statements ✓Chapter 11: Constructing 'While' Loops In Python Chapter 12: Constructing 'For Loops' In Python Programming ✓Chapter 13: Constructing Classes and Defining Objects Python 3 Programming: A Beginner Crash Course Guide to Learn Python - An Introduction to Python - How to Design a Software - Learn How to Create Data Types and Variables - Conditional Statements - Create and modify Data Structures in Python - Manipulate and Working with Strings - How to Use Files - Automate Coding Tasks

By Building Custom Python Functions - Solutions Learn Java: A Crash Course Guide to Learn Java in 1 Week * The fundamentals of Java * How to program the right way, cutting out the useless fluff! * Use arrays and classes for managing program data. * Write programs that use loops to perform repetitive tasks. * Design and write procedural programs that use methods. * Understanding Java Variables, Arrays, Loops, and Conditional Statements * Use if and switch statements to make decisions in your programs. * Learn the concept of Object Oriented Programming (from fundamentals to advanced) * How to understand and write simple Java programs * And much, much more! Let's begin our learning. Excel 2016: A Comprehensive Beginner's Guide to Microsoft Excel 2016Inside, you are going to find topics that include: ✓ Excel Essentials ✓ The Cell ✓ How to create Formulas ✓ How to use Functions. ✓ How To Managing Data, ✓ How To create Charts. ✓ and much more! Get your copy today!

A Primer on Scientific Programming with Python

Penetration Testing

This is the eBook of the printed book and may not include any media, website access codes, or print supplements that may come packaged with the bound book.

Conquer today’s Windows 10—from the inside out! Dive into Windows 10—and really put your Windows expertise to work. Focusing on the most powerful and innovative features of Windows 10, this supremely organized reference packs hundreds of timesaving solutions, tips, and workarounds—all fully reflecting the major Windows 10 Anniversary Update. From new Cortana and Microsoft Edge enhancements to the latest security and virtualization features, you’ll discover how experts tackle today’s essential tasks—and challenge yourself to new levels of mastery. Install, configure, and personalize the newest versions of Windows 10 Understand Microsoft’s revamped activation and upgrade processes Discover major Microsoft Edge enhancements, including new support for extensions Use today’s improved Cortana services to perform tasks, set reminders, and retrieve information Make the most of the improved ink, voice, touch, and gesture support in Windows 10 Help secure Windows 10 in business with Windows Hello and Azure AD Deploy, use, and manage new Universal Windows Platform (UWP) apps Take advantage of new entertainment options, including Groove Music Pass subscriptions and connections to your Xbox One console Manage files in the cloud with Microsoft OneDrive and OneDrive for Business Use the improved Windows 10 Mail and Calendar apps and the new Skype app Fine-tune performance and troubleshoot crashes Master high-efficiency tools for managing Windows 10 in the enterprise Leverage advanced Hyper-V features, including Secure Boot, TPMs, nested virtualization, and containers In addition, this book is part of the Current Book Service from Microsoft Press. Books in this program will receive periodic

updates to address significant software changes for 12 to 18 months following the original publication date via a free Web Edition. Learn more at https://www.microsoftpressstore.com/cbs.

The Art of Network Penetration Testing

Trust the best-selling Cert Guide series from Pearson IT Certification to help you learn, prepare, and practice for exam success. Cert Guides are built with the objective of providing assessment, review, and practice to help ensure you are fully prepared for your certification exam. Master Red Hat RHCSA (EX200) and RHCE (EX300) exam topics Assess your knowledge with chapter-opening quizzes Review key concepts with exam preparation tasks Test yourself with 4 practice exams (2 RHCSA and 2 RHCE) Gain expertise and knowledge using the companion website, which contains over 40 interactive exercises, 4 advanced CLI simulations, 40 interactive quizzes and glossary quizzes (one for each chapter), 3 virtual machines and more. Red Hat RHCSA/RHCE 7 Cert Guide presents you with an organized test preparation routine through the use of proven series elements and techniques. “Do I Know This Already?” quizzes open each chapter and allow you to decide how much time you need to spend on each section. Exam topic lists make referencing easy. Chapter-ending labs help you drill on key concepts you must know thoroughly. Red Hat RHCSA/RHCE 7, Premium Edition eBook and Practice Test focuses specifically on the objectives for the newest Red Hat RHCSA (EX200)

and RHCE (EX300) exams reflecting Red Hat Enterprise Linux 7. Expert Linux trainer and consultant Sander van Vugt shares preparation hints and test-taking tips, helping you identify areas of weakness and improve both your conceptual knowledge and hands-on skills. Material is presented in a concise manner, focusing on increasing your understanding and retention of exam topics. Well-regarded for its level of detail, assessment features, comprehensive design scenarios, and challenging review questions and exercises, this study guide helps you master the concepts and techniques that will allow you to succeed on the exam the first time. This study guide helps you master all the topics on the new RHCSA (EX200) and RHCE (EX300) exams, including Part 1: RHCSA Basic System Management: Installation, tools, text files, server connections; user, group, and permissions management; network configuration Operating Running Systems: Process management, VMs, package installation, task scheduling, logging, managing partitions and LVM logical volumes Advanced System Administration: Basic kernel management, basic Apache server configuration, boot procedures/troubleshooting Managing Network Services: Using Kickstart; managing SELinux; configuring firewalls, remote mounts, FTP, and time services Part 2: RHCE System Configuration/Management: External authentication/authorization, iSCSI SANs, performance reporting, optimization, logging, routing/advanced networking, Bash scripting System Security: Configuring firewalls, advanced Apache services, DNS, MariaDB, NFS, Samba, SMTP, SSH, and time synchronization

The Practice of System and Network Administration

This book provides readers with an introductory resource for learning how to create compelling games using the open source Python programming language and Pygame games development library. Authored by industry veteran and Python expert Will McGugan, readers are treated to a comprehensive, practical introduction to games development using these popular technologies. They can also capitalize upon numerous tips and tricks the author has accumulated over his career creating games for some of the world's largest gaming developers.

Learning Kali Linux

A thrilling cyber-doomsday action/adventure novel that's Ally Carter meets GAMER ARMY.

How Linux Works, 2nd Edition

Leverage Wireshark, Lua and Metasploit to solve any securitychallenge Wireshark is arguably one of the most versatile networking toolsavailable, allowing microscopic examination of almost any kind ofnetwork activity. This book is designed to help you quicklynavigate and leverage Wireshark effectively, with a

primer forexploring the Wireshark Lua API as well as an introduction to theMetasploit Framework. Wireshark for Security Professionals covers bothoffensive and defensive concepts that can be applied to any Infosecposition, providing detailed, advanced content demonstrating thefull potential of the Wireshark tool. Coverage includes theWireshark Lua API, Networking and Metasploit fundamentals, plusimportant foundational security concepts explained in a practicalmanner. You are guided through full usage of Wireshark, frominstallation to everyday use, including how to surreptitiouslycapture packets using advanced MiTM techniques. Practicaldemonstrations integrate Metasploit and Wireshark demonstrating howthese tools can be used together, with detailed explanations andcases that illustrate the concepts at work. These concepts can beequally useful if you are performing offensive reverse engineeringor performing incident response and network forensics. Lua sourcecode is provided, and you can download virtual lab environments aswell as PCAPs allowing them to follow along and gain hands onexperience. The final chapter includes a practical case study thatexpands upon the topics presented to provide a cohesive example ofhow to leverage Wireshark in a real world scenario. Understand the basics of Wireshark and Metasploit within thesecurity space Integrate Lua scripting to extend Wireshark and perform packetanalysis Learn the technical details behind common networkexploitation Packet analysis in the context of both offensive and defensivesecurity research Wireshark is the standard network analysis tool used across manyindustries due to its powerful feature set and support for

numerousprotocols. When used effectively, it becomes an invaluable tool forany security professional, however the learning curve can be steep.Climb the curve more quickly with the expert insight andcomprehensive coverage inWireshark for SecurityProfessionals.

Learn Ethical Hacking from Scratch

Step-by-step tutorials on deep learning neural networks for computer vision in python with Keras.

Learning Malware Analysis

In today's data driven biology, programming knowledge is essential in turning ideas into testable hypothesis. Based on the author’s extensive experience, Python for Bioinformatics, Second Edition helps biologists get to grips with the basics of software development. Requiring no prior knowledge of programming-related concepts, the book focuses on the easy-to-use, yet powerful, Python computer language. This new edition is updated throughout to Python 3 and is designed not just to help scientists master the basics, but to do more in less time and in a reproducible way. New developments added in this edition include NoSQL databases, the Anaconda Python distribution, graphical libraries like Bokeh, and

the use of Github for collaborative development.

Programming: 4 Manuscripts in 1 Book: Python for Beginners, Python 3 Guide, Learn Java, Excel 2016

Discover all the security risks and exploits that can threateniOS-based mobile devices iOS is Apple's mobile operating system for the iPhone and iPad.With the introduction of iOS5, many security issues have come tolight. This book explains and discusses them all. The award-winningauthor team, experts in Mac and iOS security, examines thevulnerabilities and the internals of iOS to show how attacks can bemitigated. The book explains how the operating system works, itsoverall security architecture, and the security risks associatedwith it, as well as exploits, rootkits, and other payloadsdeveloped for it. Covers iOS security architecture, vulnerability hunting,exploit writing, and how iOS jailbreaks work Explores iOS enterprise and encryption, code signing and memoryprotection, sandboxing, iPhone fuzzing, exploitation, ROP payloads,and baseband attacks Also examines kernel debugging and exploitation Companion website includes source code and tools to facilitateyour efforts iOS Hacker's Handbook arms you with the tools needed toidentify, understand, and foil iOS attacks.

System Programmer's Guide to Z/OS System Logger

Financial Risk Modelling and Portfolio Optimization with R, 2nd Edition Bernhard Pfaff, Invesco Global Asset Allocation, Germany A must have text for risk modelling and portfolio optimization using R. This book introduces the latest techniques advocated for measuring financial market risk and portfolio optimization, and provides a plethora of R code examples that enable the reader to replicate the results featured throughout the book. This edition has been extensively revised to include new topics on risk surfaces and probabilistic utility optimization as well as an extended introduction to R language. Financial Risk Modelling and Portfolio Optimization with R: Demonstrates techniques in modelling financial risks and applying portfolio optimization techniques as well as recent advances in the field. Introduces stylized facts, loss function and risk measures, conditional and unconditional modelling of risk; extreme value theory, generalized hyperbolic distribution, volatility modelling and concepts for capturing dependencies. Explores portfolio risk concepts and optimization with risk constraints. Is accompanied by a supporting website featuring examples and case studies in R. Includes updated list of R packages for enabling the reader to replicate the results in the book. Graduate and postgraduate students in finance, economics, risk management as well as practitioners in finance and portfolio optimization will find this book beneficial. It also serves well as an accompanying text in computer-lab classes and is therefore suitable for self-study.

Python for Data Analysis

Learn to build amazing robotic projects using the powerful BeagleBone Black. About This Book Push your creativity to the limit through complex, diverse, and fascinating projects Develop applications with the BeagleBone Black and open source Linux software Sharpen your expertise in making sophisticated electronic devices Who This Book Is For This Learning Path is aimed at hobbyists who want to do creative projects that make their life easier and also push the boundaries of what can be done with the BeagleBone Black. This Learning Path's projects are for the aspiring maker, casual programmer, and budding engineer or tinkerer. You'll need some programming knowledge, and experience of working with mechanical systems to get the complete experience from this Learning Path. What You Will Learn Set up and run the BeagleBone Black for the first time Get to know the basics of microcomputing and Linux using the command line and easy kernel mods Develop a simple web interface with a LAMP platform Prepare complex web interfaces in JavaScript and get to know how to stream video data from a webcam Find out how to use a GPS to determine where your sailboat is, and then get the bearing and distance to a new waypoint Use a wind sensor to sail your boat effectively both with and against the wind Build an underwater ROV to explore the underwater world See how to build an autonomous Quadcopter In Detail BeagleBone is a microboard PC that runs Linux. It can connect to the Internet and run OSes such as Android and Ubuntu. You can transform this tiny device into a brain for an embedded application or an endless variety of electronic inventions

and prototypes. This Learning Path starts off by teaching you how to program the BeagleBone. You will create introductory projects to get yourselves acquainted with all the nitty gritty. Then we'll focus on a series of projects that are aimed at hobbyists like you and encompass the areas of home automation and robotics. With each project, we'll teach you how to connect several sensors and an actuator to the BeagleBone Black. We'll also create robots for land, sea, and water. Yes, really! The books used in this Learning Path are: BeagleBone Black Cookbook BeagleBone Home Automation Blueprints Mastering BeagleBone Robotics Style and approach This practical guide transforms complex and confusing pieces of technology to become accessible with easy- to-succeed instructions. Through clear, concise examples, you will quickly get to grips with the core concepts needed to develop home automation applications with the BeagleBone Black.

The Zope Book

Learn how to hack systems like black hat hackers and secure them like security experts Key Features Understand how computer systems work and their vulnerabilities Exploit weaknesses and hack into machines to test their security Learn how to secure systems from hackers Book Description This book starts with the basics of ethical hacking, how to practice hacking safely and legally, and how to install and interact with Kali Linux and the Linux terminal. You will explore network hacking, where you will see how to test the security of wired and wireless

networks. You'll also learn how to crack the password for any Wi-Fi network (whether it uses WEP, WPA, or WPA2) and spy on the connected devices. Moving on, you will discover how to gain access to remote computer systems using client-side and server-side attacks. You will also get the hang of post-exploitation techniques, including remotely controlling and interacting with the systems that you compromised. Towards the end of the book, you will be able to pick up web application hacking techniques. You'll see how to discover, exploit, and prevent a number of website vulnerabilities, such as XSS and SQL injections. The attacks covered are practical techniques that work against real systems and are purely for educational purposes. At the end of each section, you will learn how to detect, prevent, and secure systems from these attacks. What you will learn Understand ethical hacking and the different fields and types of hackers Set up a penetration testing lab to practice safe and legal hacking Explore Linux basics, commands, and how to interact with the terminal Access password-protected networks and spy on connected clients Use server and client-side attacks to hack and control remote computers Control a hacked system remotely and use it to hack other systems Discover, exploit, and prevent a number of web application vulnerabilities such as XSS and SQL injections Who this book is for Learning Ethical Hacking from Scratch is for anyone interested in learning how to hack and test the security of systems like professional hackers and security experts.

Windows 10 Inside Out (includes Current Book Service)

Cleo's natural singing voice isn't the best... in fact, it's awful! But when the Full Moon appears, Cleo entrances Lewis, Byron, Zane and the other boys in the neighbourhood with her beautiful singing. In the midst of her new-found siren status, Cleo shares a special moment with Lewis. But when the moon sets, will they remember their kiss in the light of day?

Complete A+ Guide to IT Hardware and Software

Hacking and Penetration Testing with Low Power Devices shows you how to perform penetration tests using small, low-powered devices that are easily hidden and may be battery-powered. It shows how to use an army of devices, costing less than you might spend on a laptop, from distances of a mile or more. Hacking and Penetration Testing with Low Power Devices shows how to use devices running a version of The Deck, a full-featured penetration testing and forensics Linux distribution, and can run for days or weeks on batteries due to their low power consumption. Author Philip Polstra shows how to use various configurations, including a device the size of a deck of cards that can easily be attached to the back of a computer. While each device running The Deck is a full-featured pen-testing platform, connecting systems together via 802.15.3 networking gives you even more power and flexibility. This reference teaches you how to construct and power these devices, install operating systems, and fill out your toolbox of small

low-power devices with hundreds of tools and scripts from the book's companion website. Hacking and Pen Testing with Low Power Devices puts all these tools into your hands and will help keep you at the top of your game performing cutting-edge pen tests from anywhere in the world! Understand how to plan and execute an effective penetration test using an army of low-power devices Learn how to configure and use open-source tools and easy-to-construct low-power devices Leverage IEEE 802.15.4 networking to perform penetration tests from up to a mile away, or use 802.15.4 gateways to perform pen tests from anywhere in the world Access penetration testing operating systems with hundreds of tools and scripts on the book's companion web site

Python for Data Analysis

Discover network vulnerabilities and threats to design effective network security strategies Key Features Plunge into scanning techniques using the most popular tools Effective vulnerability assessment techniques to safeguard network infrastructure Explore the Nmap Scripting Engine (NSE) and the features used for port and vulnerability scanning Book Description Network scanning is a discipline of network security that identifies active hosts on networks and determining whether there are any vulnerabilities that could be exploited. Nessus and Nmap are among the top tools that enable you to scan your network for vulnerabilities and open ports, which can be used as back doors into a network. Network

Scanning Cookbook contains recipes for configuring these tools in your infrastructure that get you started with scanning ports, services, and devices in your network. As you progress through the chapters, you will learn how to carry out various key scanning tasks, such as firewall detection, OS detection, and access management, and will look at problems related to vulnerability scanning and exploitation in the network. The book also contains recipes for assessing remote services and the security risks that they bring to a network infrastructure. By the end of the book, you will be familiar with industry-grade tools for network scanning, and techniques for vulnerability scanning and network protection. What you will learn Install and configure Nmap and Nessus in your network infrastructure Perform host discovery to identify network devices Explore best practices for vulnerability scanning and risk assessment Understand network enumeration with Nessus and Nmap Carry out configuration audit using Nessus for various platforms Write custom Nessus and Nmap scripts on your own Who this book is for If you're a network engineer or information security professional wanting to protect your networks and perform advanced scanning and remediation for your network infrastructure, this book is for you.

Wireshark for Security Professionals

Windows 7 Inside Out

This IBM® Redbooks publication is a comprehensive guide that covers the IBM AIX® operating system (OS) layout capabilities, distinct features, system installation, and maintenance, which includes AIX security, trusted environment, and compliance integration, with the benefits of IBM Power Virtualization Management (PowerVM®) and IBM Power Virtualization Center (IBM PowerVC), which includes cloud capabilities and automation types. The objective of this book is to introduce IBM AIX modernization features and integration with different environments: General AIX enhancements AIX Live Kernel Update individually or using Network Installation Manager (NIM) AIX security features and integration AIX networking enhancements PowerVC integration and features for cloud environments AIX deployment using IBM Terraform and IBM Cloud Automation Manager AIX automation that uses configuration management tools PowerVM enhancements and features Latest disaster recovery (DR) solutions AIX Logical Volume Manager (LVM) and Enhanced Journaled File System (JFS2) AIX installation and maintenance techniques

Microtimes

By its very nature, Unix is a " power tools " environment. Even beginning Unix

users quickly grasp that immense power exists in shell programming, aliases and history mechanisms, and various editing tools. Nonetheless, few users ever really master the power available to them with Unix. There is just too much to learn! Unix Power Tools, Third Edition, literally contains thousands of tips, scripts, and techniques that make using Unix easier, more effective, and even more fun. This book is organized into hundreds of short articles with plenty of references to other sections that keep you flipping from new article to new article. You'll find the book hard to put down as you uncover one interesting tip after another. With the growing popularity of Linux and the advent of Mac OS X, Unix has metamorphosed into something new and exciting. With Unix no longer perceived as a difficult operating system, more and more users are discovering its advantages for the first time. The latest edition of this best-selling favorite is loaded with advice about almost every aspect of Unix, covering all the new technologies that users need to know. In addition to vital information on Linux, Mac OS X, and BSD, Unix Power Tools, Third Edition, now offers more coverage of bcash, zsh, and new shells, along with discussions about modern utilities and applications. Several sections focus on security and Internet access, and there is a new chapter on access to Unix from Windows, addressing the heterogeneous nature of systems today. You'll also find expanded coverage of software installation and packaging, as well as basic information on Perl and Python. The book's accompanying web site provides some of the best software available to Unix users, which you can download and add to your own set of power tools. Whether you are a newcomer or a Unix power user,

you'll find yourself thumbing through the gold mine of information in this new edition of Unix Power Tools to add to your store of knowledge. Want to try something new? Check this book first, and you're sure to find a tip or trick that will prevent you from learning things the hard way.

The Hacker's Key

This book revisits many of the problems encountered in introductory quantum mechanics, focusing on computer implementations for finding and visualizing analytical and numerical solutions. It subsequently uses these implementations as building blocks to solve more complex problems, such as coherent laser-driven dynamics in the Rubidium hyperfine structure or the Rashba interaction of an electron moving in 2D. The simulations are highlighted using the programming language Mathematica. No prior knowledge of Mathematica is needed; alternatives, such as Matlab, Python, or Maple, can also be used.

Beginning Game Development with Python and Pygame

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.

Using Mathematica for Quantum Mechanics

The Zope Book, written by the experts who developed Zope, is a guide to building dynamic Web applications using Zope. Authors Amos Latteier and Michel Pelletier teach you how to utilize Zope to write Web pages, program Web scripts, use

databases, manage dynamic content, perform collaborative Web development tasks, plus much more. Whether you are new to Zope or are a skilled user, this current and comprehensive reference is designed to introduce you to Zope and its uses and teaches you how it differs from other Web application servers. From installation and advanced features, such as ZClasses, to using Zope with relational databases, or scripting with Perl and Python, The Zope Book provides the instruction you need.

Python for Bioinformatics

With more than 600 security tools in its arsenal, the Kali Linux distribution can be overwhelming. Experienced and aspiring security professionals alike may find it challenging to select the most appropriate tool for conducting a given test. This practical book covers Kali's expansive security capabilities and helps you identify the tools you need to conduct a wide range of security tests and penetration tests. You'll also explore the vulnerabilities that make those tests necessary. Author Ric Messier takes you through the foundations of Kali Linux and explains methods for conducting tests on networks, web applications, wireless security, password vulnerability, and more. You'll discover different techniques for extending Kali tools and creating your own toolset. Learn tools for stress testing network stacks and applications Perform network reconnaissance to determine what's available to attackers Execute penetration tests using automated exploit tools such as

Metasploit Use cracking tools to see if passwords meet complexity requirements Test wireless capabilities by injecting frames and cracking passwords Assess web application vulnerabilities with automated or proxy-based tools Create advanced attack techniques by extending Kali tools or developing your own Use Kali Linux to generate reports once testing is complete

Siren Status

This book describes the new generation of discrete choice methods, focusing on the many advances that are made possible by simulation. Researchers use these statistical methods to examine the choices that consumers, households, firms, and other agents make. Each of the major models is covered: logit, generalized extreme value, or GEV (including nested and cross-nested logits), probit, and mixed logit, plus a variety of specifications that build on these basics. Simulation-assisted estimation procedures are investigated and compared, including maximum stimulated likelihood, method of simulated moments, and method of simulated scores. Procedures for drawing from densities are described, including variance reduction techniques such as anithetics and Halton draws. Recent advances in Bayesian procedures are explored, including the use of the Metropolis-Hastings algorithm and its variant Gibbs sampling. The second edition adds chapters on endogeneity and expectation-maximization (EM) algorithms. No other book incorporates all these fields, which have arisen in the past 25 years. The

procedures are applicable in many fields, including energy, transportation, environmental studies, health, labor, and marketing.

IBM Spectrum Protect Plus Practical Guidance for Deployment, Configuration, and Usage

Gain hands-on experience with HDF5 for storing scientific data in Python. This practical guide quickly gets you up to speed on the details, best practices, and pitfalls of using HDF5 to archive and share numerical datasets ranging in size from gigabytes to terabytes. Through real-world examples and practical exercises, you'll explore topics such as scientific datasets, hierarchically organized groups, user-defined metadata, and interoperable files. Examples are applicable for users of both Python 2 and Python 3. If you're familiar with the basics of Python data analysis, this is an ideal introduction to HDF5. Get set up with HDF5 tools and create your first HDF5 file Work with datasets by learning the HDF5 Dataset object Understand advanced features like dataset chunking and compression Learn how to work with HDF5's hierarchical structure, using groups Create self-describing files by adding metadata with HDF5 attributes Take advantage of HDF5's type system to create interoperable files Express relationships among data with references, named types, and dimension scales Discover how Python mechanisms for writing parallel code interact with HDF5

Network Scanning Cookbook

Numerical Methods in Engineering with Python, a student text, and a reference for practicing engineers.

Linux Basics for Hackers

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

IBM AIX Enhancements and Modernization

Explaining how to use the new features of Windows 7, a comprehensive manual details hundreds of timesaving solutions, troubleshooting tips, and workarounds, along with information on such topics as Internet Explorer 8, Windows Media Center, networking, and security.

BeagleBone: Creative Projects for Hobbyists

A guide to Python, the object-oriented scripting language, discusses the use of Python in Internet and web programming; address Python's C intergration tools; and features many examples that expand as new topics are introduced. Original. (Intermediate/Advanced)

Hacking and Penetration Testing with Low Power Devices

Unlike some operating systems, Linux doesn’t try to hide the important bits from you—it gives you full control of your computer. But to truly master Linux, you need

to understand its internals, like how the system boots, how networking works, and what the kernel actually does. In this completely revised second edition of the perennial best seller How Linux Works, author Brian Ward makes the concepts behind Linux internals accessible to anyone curious about the inner workings of the operating system. Inside, you'll find the kind of knowledge that normally comes from years of experience doing things the hard way. You'll learn: –How Linux boots, from boot loaders to init implementations (systemd, Upstart, and System V) –How the kernel manages devices, device drivers, and processes –How networking, interfaces, firewalls, and servers work –How development tools work and relate to shared libraries –How to write effective shell scripts You'll also explore the kernel and examine key system tasks inside user space, including system calls, input and output, and filesystems. With its combination of background, theory, real-world examples, and patient explanations, How Linux Works will teach you what you need to know to solve pesky problems and take control of your operating system.

Financial Risk Modelling and Portfolio Optimization with R

With 28 new chapters, the third edition of The Practice of System and Network Administration innovates yet again! Revised with thousands of updates and clarifications based on reader feedback, this new edition also incorporates DevOps strategies even for non-DevOps environments. Whether you use Linux, Unix, or Windows, this new edition describes the essential practices previously handed

down only from mentor to protégé. This wonderfully lucid, often funny cornucopia of information introduces beginners to advanced frameworks valuable for their entire career, yet is structured to help even experts through difficult projects. Other books tell you what commands to type. This book teaches you the cross-platform strategies that are timeless! DevOps techniques: Apply DevOps principles to enterprise IT infrastructure, even in environments without developers Game-changing strategies: New ways to deliver results faster with less stress Fleet management: A comprehensive guide to managing your fleet of desktops, laptops, servers and mobile devices Service management: How to design, launch, upgrade and migrate services Measurable improvement: Assess your operational effectiveness; a forty-page, pain-free assessment system you can start using today to raise the quality of all services Design guides: Best practices for networks, data centers, email, storage, monitoring, backups and more Management skills: Organization design, communication, negotiation, ethics, hiring and firing, and more Have you ever had any of these problems? Have you been surprised to discover your backup tapes are blank? Ever spent a year launching a new service only to be told the users hate it? Do you have more incoming support requests than you can handle? Do you spend more time fixing problems than building the next awesome thing? Have you suffered from a botched migration of thousands of users to a new service? Does your company rely on a computer that, if it died, can't be rebuilt? Is your network a fragile mess that breaks any time you try to improve it? Is there a periodic "hell month" that happens twice a year? Twelve

times a year? Do you find out about problems when your users call you to complain? Does your corporate “Change Review Board” terrify you? Does each division of your company have their own broken way of doing things? Do you fear that automation will replace you, or break more than it fixes? Are you underpaid and overworked? No vague “management speak” or empty platitudes. This comprehensive guide provides real solutions that prevent these problems and more!

Discrete Choice Methods with Simulation

Understand malware analysis and its practical implementation Key Features Explore the key concepts of malware analysis and memory forensics using real-world examples Learn the art of detecting, analyzing, and investigating malware threats Understand adversary tactics and techniques Book Description Malware analysis and memory forensics are powerful analysis and investigation techniques used in reverse engineering, digital forensics, and incident response. With adversaries becoming sophisticated and carrying out advanced malware attacks on critical infrastructures, data centers, and private and public organizations, detecting, responding to, and investigating such intrusions is critical to information security professionals. Malware analysis and memory forensics have become must-have skills to fight advanced malware, targeted attacks, and security breaches. This book teaches you the concepts, techniques, and tools to understand the

behavior and characteristics of malware through malware analysis. It also teaches you techniques to investigate and hunt malware using memory forensics. This book introduces you to the basics of malware analysis, and then gradually progresses into the more advanced concepts of code analysis and memory forensics. It uses real-world malware samples, infected memory images, and visual diagrams to help you gain a better understanding of the subject and to equip you with the skills required to analyze, investigate, and respond to malware-related incidents. What you will learn Create a safe and isolated lab environment for malware analysis Extract the metadata associated with malware Determine malware's interaction with the system Perform code analysis using IDA Pro and x64dbg Reverse-engineer various malware functionalities Reverse engineer and decode common encoding/encryption algorithms Reverse-engineer malware code injection and hooking techniques Investigate and hunt malware using memory forensics Who this book is for This book is for incident responders, cyber-security investigators, system administrators, malware analyst, forensic practitioners, student, or curious security professionals interested in learning malware analysis and memory forensics. Knowledge of programming languages such as C and Python is helpful but is not mandatory. If you have written few lines of code and have a basic understanding of programming concepts, you'll be able to get most out of this book.

A Practical Guide to Ubuntu Linux

The book serves as a first introduction to computer programming of scientific applications, using the high-level Python language. The exposition is example and problem-oriented, where the applications are taken from mathematics, numerical calculus, statistics, physics, biology and finance. The book teaches "Matlab-style" and procedural programming as well as object-oriented programming. High school mathematics is a required background and it is advantageous to study classical and numerical one-variable calculus in parallel with reading this book. Besides learning how to program computers, the reader will also learn how to solve mathematical problems, arising in various branches of science and engineering, with the aid of numerical methods and programming. By blending programming, mathematics and scientific applications, the book lays a solid foundation for practicing computational science. From the reviews: Langtangen does an excellent job of introducing programming as a set of skills in problem solving. He guides the reader into thinking properly about producing program logic and data structures for modeling real-world problems using objects and functions and embracing the object-oriented paradigm. Summing Up: Highly recommended. F. H. Wild III, Choice, Vol. 47 (8), April 2010 Those of us who have learned scientific programming in Python ‘on the streets’ could be a little jealous of students who have the opportunity to take a course out of Langtangen’s Primer.” John D. Cook, The Mathematical Association of America, September 2011 This book goes through Python in particular, and programming in general, via tasks that scientists will

likely perform. It contains valuable information for students new to scientific computing and would be the perfect bridge between an introduction to programming and an advanced course on numerical methods or computational science. Alex Small, IEEE, CiSE Vol. 14 (2), March /April 2012 “This fourth edition is a wonderful, inclusive textbook that covers pretty much everything one needs to know to go from zero to fairly sophisticated scientific programming in Python” Joan Horvath, Computing Reviews, March 2015

Python and HDF5

This practical, tutorial-style book uses the Kali Linux distribution to teach Linux basics with a focus on how hackers would use them. Topics include Linux command line basics, filesystems, networking, BASH basics, package management, logging, and the Linux kernel and drivers. If you're getting started along the exciting path of hacking, cybersecurity, and pentesting, Linux Basics for Hackers is an excellent first step. Using Kali Linux, an advanced penetration testing distribution of Linux, you'll learn the basics of using the Linux operating system and acquire the tools and techniques you'll need to take control of a Linux environment. First, you'll learn how to install Kali on a virtual machine and get an introduction to basic Linux concepts. Next, you'll tackle broader Linux topics like manipulating text, controlling file and directory permissions, and managing user environment variables. You'll then focus in on foundational hacking concepts like

security and anonymity and learn scripting skills with bash and Python. Practical tutorials and exercises throughout will reinforce and test your skills as you learn how to: - Cover your tracks by changing your network information and manipulating the rsyslog logging utility - Write a tool to scan for network connections, and connect and listen to wireless networks - Keep your internet activity stealthy using Tor, proxy servers, VPNs, and encrypted email - Write a bash script to scan open ports for potential targets - Use and abuse services like MySQL, Apache web server, and OpenSSH - Build your own hacking tools, such as a remote video spy camera and a password cracker Hacking is complex, and there is no single way in. Why not start at the beginning with Linux Basics for Hackers?

Unix Power Tools

Master IT hardware and software installation, configuration, repair, maintenance, and troubleshooting and fully prepare for the CompTIA® A+ Core 1 (220-1001) and Core 2 (220-1002) exams. This is your all-in-one, real-world, full-color guide to connecting, managing, and troubleshooting modern devices and systems in authentic IT scenarios. Its thorough instruction built on the CompTIA A+ Core 1 (220-1001) and Core 2 (220-1002) exam objectives includes coverage of Windows 10, Mac, Linux, Chrome OS, Android, iOS, cloud-based software, mobile and IoT devices, security, Active Directory, scripting, and other modern techniques and best practices for IT management. Award-winning instructor Cheryl Schmidt also

addresses widely-used legacy technologies—making this the definitive resource for mastering the tools and technologies you'll encounter in real IT and business environments. Schmidt's emphasis on both technical and soft skills will help you rapidly become a well-qualified, professional, and customer-friendly technician. LEARN MORE QUICKLY AND THOROUGHLY WITH THESE STUDY AND REVIEW TOOLS: Learning Objectives and chapter opening lists of CompTIA A+ Certification Exam Objectives make sure you know exactly what you'll be learning, and you cover all you need to know Hundreds of photos, figures, and tables present information in a visually compelling full-color design Practical Tech Tips provide real-world IT tech support knowledge Soft Skills best-practice advice and team-building activities in every chapter cover key tools and skills for becoming a professional, customer-friendly technician Review Questions—including true/false, multiple choice, matching, fill-in-the-blank, and open-ended questions—carefully assess your knowledge of each learning objective Thought-provoking activities help students apply and reinforce chapter content, and allow instructors to "flip" the classroom if they choose Key Terms identify exam words and phrases associated with each topic Detailed Glossary clearly defines every key term Dozens of Critical Thinking Activities take you beyond the facts to deeper understanding Chapter Summaries recap key concepts for more efficient studying Certification Exam Tips provide insight into the certification exam and preparation process

Numerical Methods in Engineering with Python

The Art of Network Penetration Testing is a guide to simulating an internal security breach. You'll take on the role of the attacker and work through every stage of a professional pentest, from information gathering to seizing control of a system and owning the network. Summary Penetration testing is about more than just getting through a perimeter firewall. The biggest security threats are inside the network, where attackers can rampage through sensitive data by exploiting weak access controls and poorly patched software. Designed for up-and-coming security professionals, The Art of Network Penetration Testing teaches you how to take over an enterprise network from the inside. It lays out every stage of an internal security assessment step-by-step, showing you how to identify weaknesses before a malicious invader can do real damage. Purchase of the print book includes a free eBook in PDF, Kindle, and ePub formats from Manning Publications. About the technology Penetration testers uncover security gaps by attacking networks exactly like malicious intruders do. To become a world-class pentester, you need to master offensive security concepts, leverage a proven methodology, and practice, practice, practice. Th is book delivers insights from security expert Royce Davis, along with a virtual testing environment you can use to hone your skills. About the book The Art of Network Penetration Testing is a guide to simulating an internal security breach. You'll take on the role of the attacker and work through every stage of a professional pentest, from information gathering to seizing control of a system and owning the network. As you brute force passwords, exploit unpatched

services, and elevate network level privileges, you'll learn where the weaknesses are—and how to take advantage of them. What's inside Set up a virtual pentest lab Exploit Windows and Linux network vulnerabilities Establish persistent re-entry to compromised targets Detail your findings in an engagement report About the reader For tech professionals. No security experience required. About the author Royce Davis has orchestrated hundreds of penetration tests, helping to secure many of the largest companies in the world. Table of Contents 1 Network Penetration Testing PHASE 1 - INFORMATION GATHERING 2 Discovering network hosts 3 Discovering network services 4 Discovering network vulnerabilities PHASE 2 - FOCUSED PENETRATION 5 Attacking vulnerable web services 6 Attacking vulnerable database services 7 Attacking unpatched services PHASE 3 - POST-EXPLOITATION AND PRIVILEGE ESCALATION 8 Windows post-exploitation 9 Linux or UNIX post-exploitation 10 Controlling the entire network PHASE 4 - DOCUMENTATION 11 Post-engagement cleanup 12 Writing a solid pentest deliverable

Red Hat RHCSA/RHCE 7 Cert Guide

The Most Complete, Easy-to-Follow Guide to Ubuntu Linux The #1 Ubuntu server resource, fully updated for Ubuntu 10.4 (Lucid Lynx)-the Long Term Support (LTS) release many companies will rely on for years! Updated JumpStarts help you set up Samba, Apache, Mail, FTP, NIS, OpenSSH, DNS, and other complex servers in

minutes Hundreds of up-to-date examples, plus comprehensive indexes that deliver instant access to answers you can trust Mark Sobell's A Practical Guide to Ubuntu Linux®, Third Edition, is the most thorough and up-to-date reference to installing, configuring, and working with Ubuntu, and also offers comprehensive coverage of servers--critical for anybody interested in unleashing the full power of Ubuntu. This edition has been fully updated for Ubuntu 10.04 (Lucid Lynx), a milestone Long Term Support (LTS) release, which Canonical will support on desktops until 2013 and on servers until 2015. Sobell walks you through every essential feature and technique, from installing Ubuntu to working with GNOME, Samba, exim4, Apache, DNS, NIS, LDAP, g ufw, firestarter, iptables, even Perl scripting. His exceptionally clear explanations demystify everything from networking to security. You'll find full chapters on running Ubuntu from the command line and desktop (GUI), administrating systems, setting up networks and Internet servers, and much more. Fully updated JumpStart sections help you get complex servers running--often in as little as five minutes. Sobell draws on his immense Linux knowledge to explain both the "hows" and the "whys" of Ubuntu. He's taught hundreds of thousands of readers and never forgets what it's like to be new to Linux. Whether you're a user, administrator, or programmer, you'll find everything you need here--now, and for many years to come. The world's most practical Ubuntu Linux book is now even more useful! This book delivers Hundreds of easy-to-use Ubuntu examples Important networking coverage, including DNS, NFS, and Cacti Coverage of crucial Ubuntu topics such as sudo and the Upstart init

daemon More detailed, usable coverage of Internet server configuration, including Apache (Web) and exim4 (email) servers State-of-the-art security techniques, including up-to-date firewall setup techniques using gufw and iptables, and a full chapter on OpenSSH A complete introduction to Perl scripting for automated administration Deeper coverage of essential admin tasks-from managing users to CUPS printing, configuring LANs to building a kernel Complete instructions on keeping Ubuntu systems up-to-date using aptitude, Synaptic, and the Software Sources window And much moreincluding a 500+ term glossary Includes DVD! Get the full version of Lucid Lynx, the latest Ubuntu LTS release!

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