

## Ssh The Secure Shell The Definitive The Definitive

Computer security is an ongoing process, a relentless contest between system administrators and intruders. A good administrator needs to stay one step ahead of any adversaries, which often involves a continuing process of education. If you're grounded in the basics of security, however, you won't necessarily want a complete treatise on the subject each time you pick up a book. Sometimes you want to get straight to the point. That's exactly what the new Linux Security Cookbook does. Rather than provide a total security solution for Linux computers, the authors present a series of easy-to-follow recipes--short, focused pieces of code that administrators can use to improve security and perform common tasks securely.The Linux Security Cookbook includes real solutions to a wide range of targeted problems, such as sending encrypted email within Emacs, restricting access to network services at particular times of day, firewalling a webserver, preventing IP spoofing, setting up key-based SSH authentication, and much more. With over 150 ready-to-use scripts and configuration files, this unique book helps administrators secure their systems without having to look up specific syntax. The book begins with recipes devised to establish a secure system, then moves on to secure day-to-day practices, and concludes with techniques to help your system stay secure.Some of the "recipes" you'll find in this book are: Controlling access to your system from firewalls down to individual services, using iptables, ipchains, xinetd, inetd, and more Monitoring your network with tcpdump, dsniff, netstat, and other tools Protecting network connections with Secure Shell (SSH) and stunnel Safeguarding email sessions with Secure Sockets Layer (SSL) Encrypting files and email messages with GnuPG Probing your own security with password crackers, nmap, and handy scripts This cookbook's proven techniques are derived from hard-won experience. Whether you're responsible for security on a home Linux system or for a large corporation, or somewhere in between, you'll find valuable, to-the-point, practical recipes for dealing with everyday security issues. This book is a system saver.

Deploy and manage today's essential services on an enterprise-class, open operating system About This Book Configure and manage Linux servers in varying scenarios and for a range of business requirements Explore the up-to-date features of CentOS using real-world scenarios See practical and extensive recipes to deploy and manage CentOS Who This Book Is For This book is for Linux professionals with basic Unix/Linux functionality experience, perhaps even having set up a server before, who want to advance their knowledge in administering various services. What You Will Learn See how to deploy CentOS easily and painlessly, even in multi-server environments Configure various methods of remote access to the server so you don't always have to be in the data center Make changes to the default configuration of many services to harden them and increase the security of the system Learn to manage DNS, emails and web servers Protect yourself from threats by monitoring and logging network intrusion and system intrusion attempts, rootkits, and viruses Take advantage of today's powerful hardware by running multiple systems using virtualization In Detail CentOS is derived from Red Hat Enterprise Linux (RHEL) sources and is widely used as a Linux server. This book will help you to better configure and manage Linux servers in varying scenarios and business requirements. Starting with installing CentOS, this book will walk you through the networking aspects of CentOS. You will then learn how to manage users and their permissions, software installs, disks, filesystems, and so on. You'll then see how to secure connection to remotely access a desktop and work with databases. Toward the end, you will find out how to manage DNS, e-mails, web servers, and more. You will also learn to detect threats by monitoring network intrusion. Finally, the book will cover virtualization techniques that will help you make the most of CentOS. Style and approach This easy-to-read cookbook is filled with practical recipes. Hands-on, task-based exercises will present you with real-world solutions to deploy and manage CentOS in varying business scenarios.

If you are a web application developer who wants to use the OpenShift platform to host your next big idea but are looking for guidance on how to achieve this, then this book is the first step you need to take. This is a very accessible cookbook where no previous knowledge of OpenShift is needed. Over 100 recipes for penetration testing using Metasploit and virtual machines Key Features Special focus on the latest operating systems, exploits, and penetration testing techniques Learn new anti-virus evasion techniques and use Metasploit to evade countermeasures Automate post exploitation with AutoRunScript Exploit Android devices, record audio and video, send and read SMS, read call logs, and much more Build and analyze Metasploit modules in Ruby Integrate Metasploit with other penetration testing tools Book Description Metasploit is the world's leading penetration testing tool and helps security and IT professionals find, exploit, and validate vulnerabilities. Metasploit allows penetration testing automation, password auditing, web application scanning, social engineering, post exploitation, evidence collection, and reporting. Metasploit's integration with InsightVM (or Nexpose), Nessus, OpenVAS, and other vulnerability scanners provides a validation solution that simplifies vulnerability prioritization and remediation reporting. Teams can collaborate in Metasploit and present their findings in consolidated reports. In this book, you will go through great recipes that will allow you to start using Metasploit effectively. With an ever increasing level of complexity, and covering everything from the fundamentals to more advanced features in Metasploit, this book is not just for beginners but also for professionals keen to master this awesome tool. You will begin by building your lab environment, setting up Metasploit, and learning how to perform intelligence gathering, threat modeling, vulnerability analysis, exploitation, and post exploitation—all inside Metasploit. You will learn how to create and customize payloads to evade anti-virus software and bypass an organization's defenses, exploit server vulnerabilities, attack client systems, compromise mobile phones, automate post exploitation, install backdoors, run keyloggers, hijack webcams, port public exploits to the framework, create your own modules, and much more. What you will learn Set up a complete penetration testing environment using Metasploit and virtual machines Master the world's leading penetration testing tool and use it in professional penetration testing Make the most of Metasploit with PostgreSQL, importing scan results, using workspaces, hosts, loot, notes, services, vulnerabilities, and exploit results Use Metasploit with the Penetration Testing Execution Standard methodology Use MSFvenom efficiently to generate payloads and backdoor files, and create shellcode Leverage Metasploit's advanced options, upgrade sessions, use proxies, use Meterpreter sleep control, and change timeouts to be stealthy Who this book is for If you are a Security professional or pentester and want to get into vulnerability exploitation and make the most of the Metasploit framework, then this book is for you. Some prior understanding of penetration testing and Metasploit is required.

A comprehensive guide to penetration testing cloud services deployed in Microsoft Azure, the popular cloud computing service provider used by numerous companies large and small. Packed with real-world examples from the author's experience as a corporate penetration tester, sample scripts from pen-tests and 'Defenders Tips' that explain how companies can reduce risk, Pentesting Azure provides a clear overview of how to effectively perform security tests so that you can provide the most accurate assessments possible.

If you are a system administrator who has some experience with virtualization and already uses VMware vCenter, but wishes to learn more, then this is the book for you. If you are looking for tips or shortcuts for common administration tasks as well as workarounds for pain points in vSphere administration, you'll find this guide useful.

Introduces more than one hundred effective ways to ensure security in a Linux, UNIX, or Windows network, covering both TCP/IP-based services and host-based security techniques, with examples of applied encryption, intrusion detections, and logging.

The Linux Enterprise Cluster explains how to take a number of inexpensive computers with limited resources, place them on a normal computer network, and install free software so that the computers act together like one powerful server. This makes it possible to build a very inexpensive and reliable business system for a small business or a large corporation. The book includes information on how to build a high-availability server pair using the Heartbeat package, how to use the Linux Virtual Server load balancing software, how to configure a reliable printing system in a Linux cluster environment, and how to build a job scheduling system in Linux with no single point of failure. The book also includes information on high availability techniques that can be used with or without a cluster, making it helpful for System Administrators even if they are not building a cluster. Anyone interested in deploying Linux in an environment where low cost computer reliability is important will find this book useful. The CD-ROM includes the Linux kernel, Idirectord software, the Mon monitoring package, the Ganglia package, OpenSSH, rsync, SystemImager, Heartbeat, and all the figures and illustrations used in the book.

[Kerberos](#)

[Build a Highly Available Cluster with Commodity Hardware and Free Software](#)

[Secure your Linux server and protect it from intruders, malware attacks, and other external threats](#)

[Using Samba](#)

[Bash Cookbook](#)

[Cisco Networking All-in-One For Dummies](#)

[Chef: Powerful Infrastructure Automation](#)

[Ssh The Secure Shell: The Definitive Guide](#)

[VMware vCenter Cookbook](#)

[SSH: The Secure Shell](#)

[JUNOS For Dummies](#)

O'Reilly's Pocket Guides have earned a reputation as inexpensive, comprehensive, and compact guides that have the stuff but not the fluff. Every page of Linux Pocket Guide lives up to this billing. It clearly explains how to get up to speed quickly on day-to-day Linux use. Once you're up and running, Linux Pocket Guide provides an easy-to-use reference that you can keep by your keyboard for those times when you want a fast, useful answer, not hours in the man pages.Linux Pocket Guide is organized the way you use Linux: by function, not just alphabetically. It's not the 'bible of Linux; it's a practical and concise guide to the options and commands you need most. It starts with general concepts like files and directories, the shell, and X windows, and then presents detailed overviews of the most essential commands, with clear examples. You'll learn each command's purpose, usage, options, location on disk, and even the RPM package that installed it.The Linux Pocket Guide is tailored to Fedora Linux--the latest spin-off of Red Hat Linux--but most of the information applies to any Linux system.Throw in a host of valuable power user tips and a friendly and accessible style, and you'll quickly find this practical, to-the-point book a small but mighty resource for Linux users.

A Primer for Computational Biology aims to provide life scientists and students the skills necessary for research in a data-rich world. The text covers accessing and using remote servers via the command-line, writing programs and pipelines for data analysis, and provides useful vocabulary for interdisciplinary work. The book is broken into three parts: Introduction to Unix/Linux: The command-line is the "natural environment" of scientific computing, and this part covers a wide range of topics, including logging in, working with files and directories, installing programs and writing scripts, and the powerful "pipe" operator for file and data manipulation. Programming in Python: Python is both a premier language for learning and a common choice in scientific software development. This part covers the basic concepts in programming (data types, if-statements and loops, functions) via examples of DNA-sequence analysis. This part also covers more complex subjects in software development such as objects and classes, modules, and APIs. Programming in R: The R language specializes in statistical data analysis, and is also quite useful for visualizing large datasets. This third part covers the basics of R as a programming language (data types, if-statements, functions, loops and when to use them) as well as techniques for large-scale, multi-test analyses. Other topics include S3 classes and data visualization with ggplot2.

Kali Linux Network Scanning Cookbook is intended for information security professionals and casual security enthusiasts alike. It will provide the foundational principles for the novice reader but will also introduce scripting techniques and in-depth analysis for the more advanced audience. Whether you are brand new to Kali Linux or a seasoned veteran, this book will aid in both understanding and ultimately mastering many of the most powerful and useful scanning techniques in the industry. It is assumed that the reader has some basic security testing experience.

If you have some experience with Zabbix and wish to take your infrastructure to the next level, then this book is for you. Before you start with Zabbix, or monitoring in general, it is best to have some basic Linux knowledge and a good understanding of snmp, virtualization, and scripting.

Raspberry Pi Cookbook for Python Programmers is written in a Cookbook format, presenting examples in the style of recipes.This allows you to go directly to your topic of interest, or follow topics throughout a chapter to gain a thorough in-depth knowledge. The aim of this book is to bring you a broad range of Python 3 examples and practical ideas which you can develop to suit your own requirements. By modifying and combining the examples to create your own projects you learn far more effectively with a much greater understanding. Each chapter is designed to become a foundation for further experimentation and discovery of the topic, providing you with the tools and information to jump right in. Readers are expected to be familiar with programming concepts and Python (where possible Python 3 is used), although beginners should manage with the help of a good Python reference book and background reading. No prior knowledge of the Raspberry Pi or electronics is required; however for the hardware sections you will need some basic electronic components/household tools to build some of the projects.

Host your own website or blog with this unique guide If you'd like to make the leap from a hosted environment to a self-hosted service, this book is for you. You may be making the move from casual blogging to professional blogging. Or, you might already be self-hosting, but want a good guide to show you how to get more out of your plan. In simple, easy-to-understand language, this helpful book breaks down all the functions of web hosting for self-hosted users, from setting up new e-mail accounts to backing up and securing your site, analyzing server logs, choosing a platform to install, and more. Breaks down the functions of web hosting for new self-hosters, including casual bloggers who may be moving into professional blogging Helps those who are already self-hosting maximize the services they are paying for Offers a one-stop, complete resource on web hosting, rather than just a few chapters, as in many blogging books Covers setting up and using e-mail accounts, working with FTP clients, backing up and securing sites, using cloud services, understanding domains and DNS, using built-in databases, and more Web Hosting For Dummies helps you take charge of your own web hosting and having fun in the process!

The first stop for your security needs when using Go, covering host, network, and cloud security for ethical hackers and defense against intrusion Key Features First introduction to Security with Golang Adopting a Blue Team/Red Team approach Take advantage of speed and inherent safety of Golang Works as an introduction to security for Golang developers Works as a guide to Golang security packages for recent Golang beginners Book Description Go is becoming more and more popular as a language for security experts. Its wide use in server and cloud environments, its speed and ease of use, and its evident capabilities for data analysis, have made it a prime choice for developers who need to think about security. Security with Go is the first Golang security book, and it is useful for both blue team and red team applications. With this book, you will learn how to write secure software, monitor your systems, secure your data, attack systems, and extract information. Defensive topics include cryptography, forensics, packet capturing, and building secure web applications. Offensive topics include brute force, port scanning, packet injection, web scraping, social engineering, and post exploitation techniques. What you will learn Learn the basic concepts and principles of secure programming Write secure Golang programs and applications Understand classic patterns of attack Write Golang scripts to defend against network-level attacks Learn how to use Golang security packages Apply and explore cryptographic methods and packages Learn the art of defending against brute force attacks Secure web and cloud applications Who this book is for Security with Go is aimed at developers with basics in Go to the level that they can write their own scripts and small programs without difficulty. Readers should be familiar with security concepts, and familiarity with Python security applications and libraries is an advantage, but not a necessity.

Are you serious about network security? Then check out SSH, the Secure Shell, which provides key-based authentication and transparent encryption for your network connections. It's reliable, robust, and reasonably easy to use, and both free and commercial implementations are widely available for most operating systems. While it doesn't solve every privacy and security problem, SSH eliminates several of them very effectively.Everything you want to know about SSH is in our second edition of SSH, The Secure Shell: The Definitive Guide. This updated book thoroughly covers the latest SSH-2 protocol for system administrators and end users interested in using this increasingly popular TCP/IP-based solution.How does it work? Whenever data is sent to the network, SSH automatically encrypts it. When data reaches its intended recipient, SSH decrypts it. The result is "transparent" encryption-users can work normally, unaware that their communications are already encrypted. SSH supports secure file transfer between computers, secure remote logins, and a unique "tunneling" capability that adds encryption to otherwise insecure network applications. With SSH, users can freely navigate the Internet, and system administrators can secure their networks or perform remote administration.Written for a wide, technical audience, SSH, The Secure Shell: The Definitive Guide covers several implementations of SSH for different operating systems and computing environments. Whether you're an individual running Linux machines at home, a corporate network administrator with thousands of users, or a PC/Mac owner who just wants a secure way to telnet or transfer files between machines, our indispensable guide has you covered. It starts with simple installation and use of SSH, and works its way to in-depth case studies on large, sensitive computer networks.No matter where or how you're shipping information, SSH, The Secure Shell: The Definitive Guide will show you how to do it securely.

[Mastering Linux Security and Hardening](#)

[Pentesting Azure Applications](#)

[CompTIA Security+ All-in-One Exam Guide \(Exam SY0-301\), 3rd Edition](#)

[Cryptography for Secure Communications](#)

[Pro OpenSSH](#)

[BeagleBone Black Cookbook](#)

[Git Pocket Guide](#)

[OpenShift Cookbook](#)

[A Primer for Computational Biology](#)

[Explore the power of Golang to secure host, web, and cloud services](#)

[Secure Shell in the Enterprise](#)

SSH, The Secure ShellThe Definitive Guide"O'Reilly Media, Inc."

Take full creative control of your web applications with Flask, the Python-based microframework. With the second edition of this hands-on book, you'll learn the framework from the ground up by developing, step-by-step, a real-world project created by author Miguel Grinberg. This refreshed edition accounts for important technology changes that have occurred in the past three years. You'll learn the framework's core functionality, as well as how to extend applications with advanced web techniques such as database migration and web service communication. The first part of each chapter provides you with reference and background for the topic in question, while the second part guides you though a hands-on implementation of the topic. If you have Python experience, this book shows you how to take advantage of the creative freedom Flask provides.

For system administrators, programmers, and end users, shell command or carefully crafted shell script can save you time and effort, or facilitate consistency and repeatability for a variety of common tasks. This cookbook provides more than 300 practical recipes for using bash, the popular Unix shell that enables you to harness and customize the power of any Unix or Linux system. Ideal for new and experienced users alike—including proficient Windows users and sysadmins—this updated second edition helps you solve a wide range of problems. You'll learn ways to handle input/output, file manipulation, program execution, administrative tasks, and many other challenges. Each recipe includes one or more scripting examples and a discussion of why the solution works. You'll find recipes for problems including: Standard output and input, and executing commands Shell variables, shell logic, and arithmetic Intermediate shell tools and advanced scripting Searching for files with find, locate, and slocate Working with dates and times Creating shell scripts for various end-user tasks Working with tasks that require parsing Writing secure shell scripts Configuring and customizing bash

A guide to the TCP/IP-based network security and privacy solution covers installation, configuration, maintenance, SSH server control, application tunneling, forced commands, port and agent forwarding, and troubleshooting.

bull; bull;Covers the new Solaris Secure Shell for all versions of Solaris bull;Shows how to secure remote logins, integrate Secure Shell into existing scripts and avoid common problems bull;Written by Jason Reid, a member of the Solaris System Test group at Sun Microsystems, Inc.

Kerberos, the single sign-on authentication system originally developed at MIT, deserves its name. It's a faithful watchdog that keeps intruders out of your networks. But it has been equally fierce to system administrators, for whom the complexity of Kerberos is legendary. Single sign-on is the holy grail of network administration, and Kerberos is the only game in town. Microsoft, by integrating Kerberos into Active Directory in Windows 2000 and 2003, has extended the reach of Kerberos to all networks large or small. Kerberos makes your network more secure and more convenient for users by providing a single authentication system that works across the entire network. One username; one password; one login is all you need. Fortunately, help for administrators is on the way. Kerberos: The Definitive Guide shows you how to implement Kerberos for secure authentication. In addition to covering the basic principles behind cryptographic authentication, it covers everything from basic installation to advanced topics like cross-realm authentication, defending against attacks on Kerberos, and troubleshooting. In addition to covering Microsoft's Active Directory implementation, Kerberos: The Definitive Guide covers both major implementations of Kerberos for Unix and Linux: MIT and Heimdal. It shows you how to set up Mac OS X as a Kerberos client. The book also covers both versions of the Kerberos protocol that are still in use: Kerberos 4 (now obsolete) and Kerberos 5, paying special attention to the integration between the different protocols, and between Unix and Windows implementations. If you've been avoiding Kerberos because it's confusing and poorly documented, it's time to get on board! This book shows you how to put Kerberos authentication to work on your Windows and Unix systems.

A helpful guide on all things Cisco Do you wish that the complex topics of routers, switches, and networking could be presented in a simple, understandable presentation? With Cisco Networking All-in-One For Dummies, they are! This expansive reference is packed with all the information you need to learn to use Cisco routers and switches to develop and manage secure Cisco networks. This straightforward-by-fun guide offers expansive coverage of Cisco and breaks down intricate subjects such as networking, virtualization, and database technologies into easily digestible pieces. Drills down complex subjects concerning Cisco networking into easy-to-understand, straightforward coverage Shares best practices for utilizing Cisco switches and routers to implement, secure, and optimize Cisco networks Reviews Cisco networking solutions and products, securing Cisco networks, and optimizing Cisco networks Details how to design and implement Cisco networks Whether you're new to Cisco networking products and services or an experienced professional looking to refresh your knowledge about Cisco, this For Dummies guide provides you with the coverage, solutions, and best practices you need.

Over 60 recipes and solutions for inventors, makers, and budding engineers to create projects using the BeagleBone Black About This Book Learn how to develop applications with the BeagleBone Black and open source Linux software Sharpen your expertise in making sophisticated electronic devices Explore the BeagleBone Black with this easy-to-succeed recipe format Who This Book Is For If you are a hardware, Linux, and/or microcomputing novice, or someone who wants more power and possibilities with product prototypes, electronic art projects, or embedded computing experiments, then this book is for you. It is for Internet of Things enthusiasts who want to use more sophisticated hardware than the Raspberry Pi or the Arduino can provide. Whether you are an engineering student, a DIYer, an inventor, or a budding electronics enthusiast, this book delivers accessible, easy-to-succeed instructions for using an advanced microcomputing platform. What You Will Learn Set up and run the BeagleBone Black for the first time Learn the basics of microcomputing and Linux using the command line and easy kernel mods Make introductory projects with Python, JavaScript, BoneScript, and Node.js Explore physical computing and simple circuits using buttons, LEDs, sensors, and motors Discover the unique features of the BeagleBone Black and its real-time computing functions Build intermediate level audio and video applications Assemble and add ingredients for creating Internet of Things prototypes In Detail There are many single-board controllers and computers such as Arduino, Udoo, or Raspberry Pi, which can be used to create electronic prototypes on circuit boards. However, when it comes to creating more advanced projects, BeagleBone Black provides a sophisticated alternative. Mastering the BeagleBone Black enables you to combine it with sensors and LEDs, add buttons, and marry it to a variety of add-on boards. You can transform this tiny device into the brain for an embedded application or an endless variety of electronic inventions and prototypes. With dozens of how-tos, this book kicks off with the basic steps for setting up and running the BeagleBone Black for the first time, from connecting the necessary hardware and using the command line with Linux commands to installing new software and controlling your system remotely. Following these recipes, more advanced examples take you through scripting, debugging, and working with software source files, eventually working with the Linux kernel. Subsequently, you will learn how to exploit the board's real-time functions. We will then discover exciting methods for using sound and video with the system before marching forward into an exploration of recipes for building Internet of Things projects. Finally, the book finishes with a dramatic arc upward into outer space, when you explore ways to build projects for tracking and monitoring satellites. Style and approach This comprehensive recipe book deconstructs a complex, often confusing piece of technology, and transforms it to become accessible and fun with snappy, unintimidating prose, and extensive easy-to-succeed instructions.

[The Linux Enterprise Cluster Linux Pocket Guide](#)  
[Network Security with OpenSSL](#)  
[Implementing SSH](#)  
[Zabbix Cookbook](#)  
[Metasploit Penetration Testing Cookbook](#)  
[Pro Git](#)  
[Strategies for Optimizing the Secure Shell SSH, The Secure Shell: The Definitive Guide](#)  
[CentOS 7 Server Deployment Cookbook](#)  
[SSH, the Secure Shell](#)

Learn Chef Provisioning like a boss and discover how to deploy software and manage hosts, along with engaging recipes to automate your cloud and server infrastructure with Chef. About This Book Leverage the power of Chef to transform your infrastructure into code to deploy new features in minutes Get step-by-step instructions to configure, deploy, and scale your applications Master specific Chef techniques to run an entire fleet of machines without breaking a sweat. Who This Book Is For If you are a system administrator, Linux administrator, a cloud developer, or someone who just wants to learn and apply Chef automation to your existing or new infrastructure, then this learning path will show you all you need to know. In order to get the most out of this learning path, some experience of programming or scripting languages would be useful. What You Will Learn Install Chef server on your own hosts Integrate Chef with cloud services Debug your cookbooks and Chef runs using the numerous inspection and logging facilities of Chef Extend Chef to meet your advanced needs by creating custom plugins for Knife and Ohai Create a perfect model system Use the best test-driven development methodologies In Detail Chef is a configuration management tool that turns IT infrastructure into code. Chef provides tools to manage systems at scale. This learning path takes you on a comprehensive tour of Chef's functionality, ranging from its core features to advanced development. You will be brought up to speed with what's new in Chef and how to set up your own Chef infrastructure for individuals, or small or large teams. You will learn to use the basic Chef command-line tools. We will also take you through the core concepts of managing users, applications, and your entire cloud infrastructure. You will learn the techniques of the pros by walking you through a host of step-by-step guides to solve real-world infrastructure automation challenges. You will learn to automate and document every aspect of your network, from the hardware to software, middleware, and all your containers. You will become familiar with the Chef's Provisioning tool. By the end of this course, you will be confident in how to manage your infrastructure, scale using the cloud, and extend the built-in functionality of Chef itself. The books used in this Learning Path are: 1) Chef Essentials 2) Chef Infrastructure Automation Cookbook – Second Edition 3) Mastering Chef Provisioning Style and approach This fast-paced guide covers the many facets of Chef and will teach administrators to use Chef as a birds-eye lens for their entire system. This book takes you through a host of step-by-step guides to solve real-world infrastructure automation challenges and offers elegant, time-saving solutions for a perfectly described and automated network.

Most applications these days are at least somewhat network aware, but how do you protect those applications against common network security threats? Many developers are turning to OpenSSL, an open source version of SSL/TLS, which is the most widely used protocol for secure network communications. The OpenSSL library is seeing widespread adoption for web sites that require cryptographic functions to protect a broad range of sensitive information, such as credit card numbers and other financial transactions. The library is the only free, full-featured SSL implementation for C and C++, and it can be used programmatically or from the command line to secure most TCP-based network protocols. Network Security with OpenSSL enables developers to use this protocol much more effectively. Traditionally, getting something simple done in OpenSSL could easily take weeks. This concise book gives you the guidance you need to avoid pitfalls, while allowing you to take advantage of the library's advanced features. And, instead of bogging you down in the technical details of how SSL works under the hood, this book provides only the information that is necessary to use OpenSSL safely and effectively. In step-by-step fashion, the book details the challenges in securing network communications, and shows you how to use OpenSSL tools to best meet those challenges. As a system or network administrator, you will benefit from the thorough treatment of the OpenSSL command-line interface, as well as from step-by-step directions for obtaining certificates and setting up your own certification authority. As a developer, you will further benefit from the in-depth discussions and examples of how to use OpenSSL in your own programs. Although OpenSSL is written in C, information on how to use OpenSSL with Perl, Python and PHP is also included. OpenSSL may well answer your need to protect sensitive data. If that's the case, Network Security with OpenSSL is the only guide available on the subject.

Learn how to build physical computing systems using BeagleBone Black and Python About This Book Get to grips with the fundamentals of BeagleBone Leverage Python scripts to program BeagleBone for your requirements Build four exciting projects, from home automation to a tele-controlled robot Who This Book Is For This book is intended for hobbyists and consumers who wish to create impressive projects using BeagleBone. You must be familiar with Python programming. What You Will Learn Program on BeagleBone Black using Python Interface sensors and actuators to BeagleBone Black Build your own real-time physical computing systems Connect physical computing systems to cloud servers Build your own home automation and home security system Build your own tele-controlled robot with real-time video streaming In Detail BeagleBone is a low cost, community-supported development platform to develop a variety of electronic projects. This book will introduce you to BeagleBone and get you building fun, cool, and innovative projects with it. Start with the specifications of BeagleBone Black and its operating systems, then get to grips with the GPIOs available in BeagleBone Black. Work through four types of exciting projects: building real-time physical computing systems, home automation, image processing for a security system, and building your own tele-controlled robot and learn the fundamentals of a variety of projects in a single book. By the end of this book, you will be able to write code for BeagleBone in order to operate hardware and impart decision-making capabilities with the help of efficient coding in Python. Style and approach This book is a step by step guide that will walk you through the fundamentals of building different projects using BeagleBone Black.

Be more productive and make your life easier. That's what LDAP System Administration is all about. System administrators often spend a great deal of time managing configuration information located on many different machines: usernames, passwords, printer configurations, email client configurations, and network filesystem configurations, to name a few. LDAPv3 provides tools for centralizing all of the configuration information and placing it under your control. Rather than maintaining several administrative databases (NIS, Active Directory, Samba, and NFS configuration files), you can make changes in only one place and have all your systems immediately "see" the updated information. Practically platform independent, this book uses the widely available, open source OpenLDAP 2 directory server as a premise for examples, showing you how to use it to help you manage your configuration information effectively and securely. OpenLDAP 2 ships with most Linux® distributions and Mac OS® X, and can be easily downloaded for most Unix-based systems. After introducing the workings of a directory service and the LDAP protocol, all aspects of building and installing OpenLDAP, plus key ancillary packages like SASL and OpenSSL, this book discusses: Configuration and access control Distributed directories; replication and referral Using OpenLDAP to replace NIS Using OpenLDAP to manage email configurations Using LDAP for abstraction with FTP and HTTP servers, Samba, and Radius Interoperating with different LDAP servers, including Active Directory Programming using Net::LDAP If you want to be a master of your domain, LDAP System Administration will help you get up and running quickly regardless of which LDAP version you use. After reading this book, even with no previous LDAP experience, you'll be able to integrate a directory server into essential network services such as mail, DNS, HTTP, and SMB/CIFS.

Pro Git (Second Edition) is your fully-updated guide to Git and its usage in the modern world. Git has come a long way since it was first developed by Linus Torvalds for Linux kernel development. It has taken the open source world by storm since its inception in 2005, and this book teaches you how to use it like a pro. Effective and well-implemented version control is a necessity for successful web projects, whether large or small. With this book you'll learn how to master the world of distributed version workflow, use the distributed features of Git to the full, and extend Git to meet your every need. Written by Git pros Scott Chacon and Ben Straub, Pro Git (Second Edition) builds on the hugely successful first edition, and is now fully updated for Git version 2.0, as well as including an indispensable chapter on GitHub. It's the best book for all your Git needs.

\* Authored by two Fortune 100 system administrators responsible for the architecture and deployment of OpenSSH across several hundred corporate servers. \* Covers commonplace yet often confusing deployment scenarios that come up daily in enterprise environments, large and small. \* Focuses upon the world's most prevalent SSH implementation, OpenSSH.

A comprehensive guide to mastering the art of preventing your Linux system from getting compromised. Key Features Leverage this guide to confidently deliver a system that reduces the risk of being hacked Perform a number of advanced Linux security techniques such as network service detection, user authentication, controlling special permissions, encrypting file systems, and much more Master the art of securing a Linux environment with this end-to-end practical guide Book Description This book has extensive coverage of techniques that will help prevent attackers from breaching your system, by building a much more secure Linux environment. You will learn various security techniques such as SSH hardening, network service detection, setting up firewalls, encrypting file systems, protecting user accounts, authentication processes, and so on. Moving forward, you will also develop hands-on skills with advanced Linux permissions, access control, special modes, and more. Lastly, this book will also cover best practices and troubleshooting techniques to get your work done efficiently. By the end of this book, you will be confident in delivering a system that will be much harder to compromise. What you will learn Use various techniques to prevent intruders from accessing sensitive data Prevent intruders from planting malware, and detect whether malware has been planted Prevent insiders from accessing data that they aren't authorized to access Do quick checks to see whether a computer is running network services that it doesn't need to run Learn security techniques that are common to all Linux distros, and some that are distro-specific Who this book is for If you are a systems administrator or a network engineer interested in making your Linux environment more secure, then this book is for you. Security consultants wanting to enhance their Linux security skills will also benefit from this book. Prior knowledge of Linux is mandatory. This book is the comprehensive guide to Samba administration, officially adopted by the Samba Team. Wondering how to integrate Samba's authentication with that of a Windows domain? How to get Samba to serve Microsoft Dfs shares? How to share files on Mac OS X? These and a dozen other issues of interest to system administrators are covered. A whole chapter is dedicated to troubleshooting! The range of this book knows few bounds. Using Samba takes you from basic installation and configuration -- on both the client and server side, for a wide range of systems -- to subtle details of security, cross-platform compatibility, and resource discovery that make the difference between whether users see the folder they expect or a cryptic error message. The current edition covers such advanced 3.x features as: Integration with Active Directory and OpenLDAP Migrating from Windows NT 4.0 domains to Samba Delegating administrative tasks to non-root users Central printer management Advanced file serving features, such as making use of Virtual File System (VFS) plugins. Samba is a cross-platform triumph: robust, flexible and fast, it turns a Unix or Linux system into a file and print server for Microsoft Windows network clients. This book will help you make your file and print sharing as powerful and efficient as possible. The authors delve into the internals of the Windows activities and protocols to an unprecedented degree, explaining the strengths and weaknesses of each feature in Windows domains and in Samba itself. Whether you're playing on your personal computer or an enterprise network, on one note or a full three-octave range, Using Samba will give you an efficient and secure server.

[Kali Linux Network Scanning Cookbook](#)  
[Flask Web Development](#)

[Evade antiviruses, bypass firewalls, and exploit complex environments with the most widely used penetration testing framework, 3rd Edition](#)

[Raspberry Pi Cookbook for Python Programmers](#)  
[Security with Go](#)  
[A Working Introduction](#)  
[The Definitive Guide](#)  
[Security Tools & Techniques](#)  
[BeagleBone By Example](#)  
[A File & Print Server for Linux, Unix & Mac OS X](#)

The definitive, easy-to-use guide to the popular BeagleBone board BeagleBone For Dummies is the definitive beginner's guide to using the popular BeagleBone board to learn electronics and programming. Unlike other books that require previous knowledge of electronics, Linux, and Python, this one assumes you know nothing at all, and guides you step-by-step throughout the process of getting acquainted with your BeagleBone Original or BeagleBone Black. You'll learn how to get set up, use the software, build the hardware, and code your projects, with plenty of examples to walk you through the process. You'll move carefully through your first BeagleBone project, then get ideas for branching out from there to create even better, more advanced programs. The BeagleBone is a tiny computer board – about the size of a credit card – that has all the capability of a desktop. Its affordability and ease of use has made it popular among hobbyists, hardware enthusiasts, and programmers alike, and it's time for you to join their ranks as you officially dive into the world of microcomputers. This book removes the guesswork from using the popular BeagleBone board and shows you how to get up and running in no time. Download the operating system and connect your BeagleBone Learn to navigate the desktop environment Start programming with Python and Bonescript Build your first project, and find plans for many more To learn BeagleBone, you could spend hours on the Internet and still never find the information you need, or you can get everything you need here. This book appeals to all new and inexperienced hobbyists, tinkerers, electronics gurus, hackers, budding programmers, engineers, and hardware geeks who want to learn how to get the most out of their powerful BeagleBone.

Master Wicket by example by implementing real-life solutions to every day tasks.

This pocket guide is the perfect on-the-job companion to Git, the distributed version control system. It provides a compact, readable introduction to Git for new users, as well as a reference to common commands and procedures for those of you with Git experience. Written for Git version 1.8.2, this handy task-oriented guide is organized around the basic version control functions you need, such as making commits, fixing mistakes, merging, and searching history. Examine the state of your project at earlier points in time Learn the basics of creating and making changes to a repository Create branches so many people can work on a project simultaneously Merge branches and reconcile the changes among them Clone an existing repository and share changes with push/pull commands Examine and change your repository's commit history Access remote repositories, using different network protocols Get recipes for accomplishing a variety of common tasks Official CompTIA Content! Prepare for CompTIA Security+ Exam SY0-301 with McGraw-Hill—a Gold-Level CompTIA Authorized Partner offering Official CompTIA Approved Quality Content to give you the competitive edge on exam day. Get complete coverage of all the objectives included on CompTIA Security+ exam inside this completely updated, comprehensive volume. Written by leading network security experts, this definitive guide covers exam SY0-301 in full detail. You'll find learning objectives at the beginning of each chapter, exam tips, practice exam questions, and in-depth explanations. Designed to help you pass the exam with ease, this practical resource also serves as an essential on-the-job reference. Covers all exam topics, including: General security concepts Operational organizational security Legal issues, privacy, and ethics Cryptography Public key infrastructure Standards and protocols Physical security Infrastructure security Remote access and authentication Intrusion detection systems Security baselines Types of attacks and malicious software E-mail and instant messaging Web components Disaster recovery and business continuity Risk, change, and privilege management Computer forensics Electronic content includes two full practice exams From the bestselling author of The 48 Laws of Power and The Laws of Human Nature, a vital work revealing that the secret to mastery is already within you. Each one of us has within us the potential to be a Master. Learn the secrets of the field you have chosen, submit to a rigorous apprenticeship, absorb the hidden knowledge possessed by those with years of experience, surge past competitors to surpass them in brilliance, and explode established patterns from within. Study the behaviors of Albert Einstein, Charles Darwin, Leonardo da Vinci and the nine contemporary Masters interviewed for this book. The bestselling author of The 48 Laws of Power, The Art of Seduction, and The 33 Strategies of War, Robert Greene has spent a lifetime studying the laws of power. Now, he shares the secret path to greatness. With this seminal text as a guide, readers will learn how to unlock the passion within and become masters. Are you serious about network security? Then check out SSH, the Secure Shell, which provides key-based authentication and transparent encryption for your network connections. It's reliable, robust, and reasonably easy to use, and both free and commercial implementations are widely available for most operating systems. While it doesn't solve every privacy and security problem, SSH eliminates several of them very effectively. Everything you want to know about SSH is in our second edition of SSH, The Secure Shell: The Definitive Guide. This updated book thoroughly covers the latest SSH-2 protocol for system administrators and end users interested in using this increasingly primary TCP/IP-based solution. How does it work? Whenever data is sent to the network, SSH automatically encrypts it. When data reaches its intended recipient, SSH decrypts it. The result is "transparent" encryption—users can work normally, unaware that their communications are already encrypted. SSH supports secure file transfer between computers, secure remote logins, and a unique "tunneling" capability that adds encryption to otherwise insecure network applications. With SSH, users can freely navigate the Internet, and system administrators can secure their networks or perform remote administration. Written for a wide, technical audience, SSH, The Secure Shell: The Definitive Guide covers several implementations of SSH for different operating systems and computing environments. Whether you're an individual running Linux machines at home, a corporate network administrator with thousands of users, or a PC/Mac owner who just wants a secure way to telnet or transfer files between machines, our indispensable guide has you covered. It starts with simple installation and use of SSH, and works its way to in-depth case studies on large, sensitive computer networks. No matter where or how you're shipping information, SSH, The Secure Shell: The Definitive Guide will show you how to do it securely.

[PISense 2 Cookbook](#)  
[The Definitive Guide to Testing and Securing Deployments](#)  
[Putting Directories to Work](#)  
[Developing Web Applications with Python](#)  
[Network Security Hacks](#)  
[BeagleBone For Dummies](#)  
[Mastery](#)  
[LDAP System Administration](#)  
[Linux Security Cookbook](#)  
[Solutions and Examples for Bash Users](#)  
[Web Hosting For Dummies](#)