

Ssh The Secure Shell The Definitive Guide

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.

Firewalls, Network Address Translation (NAT), network logging and accounting are all provided by Linux's Netfilter system, also known by the name of the command used to administer it, iptables. The iptables interface is the most sophisticated ever offered on Linux and makes Linux an extremely flexible system for any kind of network filtering you might do. Large sets of filtering rules can be grouped in ways that makes it easy to test them and turn them on and off. Do you watch for all types of ICMP traffic--some of them quite dangerous? Can you take advantage of stateful filtering to simplify the management of TCP connections? Would you like to track how much traffic of various types you get? This pocket reference will help you at those critical moments when someone asks you to open or close a port in a hurry, either to enable some important traffic or to block an attack. The book will keep the subtle syntax straight and help you remember all the values you have to enter in order to be as secure as possible. The book has an introductory section that describes applications, followed by a reference/encyclopaedic section with all the matches and targets arranged alphabetically.

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.

* 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 worlds most prevalent SSH implementation, OpenSSH.

From the authors of the bestselling E-Mail Virus Protection Handbook! The Linux operating system continues to gain market share based largely on its reputation as being the most secure operating system available. The challenge faced by system administrators installing Linux is that it is secure only if installed and configured properly, constantly and meticulously updated, and carefully integrated with a wide variety of Open Source security tools. The fact that Linux source code is readily available to every hacker means that system administrators must continually learn security and anti-hacker techniques. Hack Proofing Linux will provide system administrators with all of the techniques necessary to properly configure and maintain Linux systems and counter malicious attacks. Linux operating systems and Open Source security tools are incredibly powerful, complex, and notoriously under-documented - this book addresses a real need Uses forensics-based analysis to give the reader an insight to the mind of a hacker

The BeagleBone is a tiny computer board about the size of a credit card and which has all the capability of a desktop. This volume guides you step-by-step throughout the process of getting acquainted with your BeagleBone Original or BeagleBoneBlack. 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 even better, more advanced programs.

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, dsniiff, 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.

'Machiavelli has a new rival, and Sun-tzu had better watch his back' - New York Times Around the globe, people are facing the same problem - that we are born as individuals but are forced to conform to the rules of society if we want to succeed. To see our uniqueness expressed in our achievements, we must first learn the rules - and then how to change them completely. Charles Darwin began as an underachieving schoolboy, Leonardo da Vinci as an illegitimate outcast. The secret of their eventual greatness lies in a 'rigorous apprenticeship': by paying close and careful attention, they learnt to master the 'hidden codes' which determine ultimate success or failure. Then, they rewrote the rules as a reflection of their own individuality, blasting previous patterns of achievement open from within. Told through Robert Greene's signature blend of historical anecdote and psychological insight and drawing on interviews with world leaders, Mastery builds on the strategies outlined in The 48 Laws of Power to provide a practical guide to greatness - and how to start living by your own rules. From the internationally bestselling author of The 48 Laws of Power, The Art Of Seduction, and The 33 Strategies Of War.

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

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.

Addressing the firewall capabilities of Linux, a handbook for security professionals describes the Netfilter infrastructure in the Linux kernel and explains how to use Netfilter as an intrusion detection system by integrating it with custom open source software and Snort rulesets, discussin such topics as Linux firewall log analysis and policies, passive network authentication and authorization, and more. Original. (Intermediate)

Pluggable Authentication Modules: Threat or Menace? PAM is one of the most misunderstood parts of systems administration. Many sysadmins live with authentication problems rather than risk making them worse. PAM's very nature makes it unlike any other Unix access control system. If you have PAM misery or PAM mysteries, you need PAM Mastery! With PAM Mastery, you'll understand: · the different versions of PAM · the intricacies of Linux-PAM and OpenPAM · how PAM policies make decisions · how to debug PAM · the most frequently seen PAM modules · Linux-PAM extended controls and substacks · time-based one-time passwords · using SSH keys for more than SSH · password quality testing · policies from CentOS, Debian, and FreeBSD · and more! Transform PAM from a headache to an ally with PAM Mastery.

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.

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.

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.

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.

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.

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.

This book constitutes the refereed proceedings of the 13th IMA International Conference on Cryptography and Coding, IMACC 2011, held in Oxford, UK in December 2011. The 27 revised full papers presented together with one invited contribution were carefully reviewed and selected from 57 submissions. The papers cover a wide range of topics in the field of mathematics and computer science, including coding theory, homomorphic encryption, symmetric and public key cryptosystems, cryptographic functions and protocols, efficient pairing and scalar multiplication implementation, knowledge proof, and security analysis.

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.

Unlock the secrets of the Terminal and discover how this powerful tool solves problems the Finder can't handle. With this handy guide, you'll learn commands for a variety of tasks, such as killing programs that refuse to quit, renaming a large batch of files in seconds, or running jobs in the background while you do other work. Get started with an easy-to-understand overview of the Terminal and its partner, the shell. Then dive into commands neatly arranged into two dozen categories, including directory operations, file comparisons, and network connections. Each command includes a concise description of its purpose and features. Log into your Mac from remote locations Search and modify files in powerful ways Schedule jobs for particular days and times Let several people use one Mac at the same time Compress and uncompress files in a variety of formats View and manipulate Mac OS X processes Combine multiple commands to perform complex operations Download and install additional commands from the Internet

The best-selling sysadmin text, now revised and updated! SSH Mastery is the industry standard work on using Secure Shell on Unix-like systems

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.

Provides readers with end-to-end shell scripts that can be used to automate repetitive tasks and solve real-world system administration problems Targets the specific command structure for four popular UNIX systems: Solaris, Linux, AIX, and HP-UX Illustrates dozens of example tasks, presenting the proper command syntax and analyzing the performance gain or loss using various control structure techniques Web site includes all the shell scripts used in the book

Learn the skills to complete the full installation, configuration, and maintenance of an enterprise class internet server, no matter what Unix-like operating system you prefer. This book will rapidly guide you towards real system administration, with clear explanations along the way. After a chapter explaining the most important Unix basics, you will start with a vanilla server as delivered by a hosting provider and by the end of the book, you will have a fully functional and well-

secured enterprise class internet server. You will also be equipped with the expertise needed to keep your server secured and up to date. All configuration examples are given for FreeBSD, Debian and CentOS, so you are free to choose your operating system. No single blueprint exists for an internet server, and an important part of the work of a system administrator consists of analyzing, interpreting and implementing specific wishes, demands and restrictions from different departments and viewpoints within an organization. Practical Internet Server Configuration provides the information you need to succeed as a sysadmin. What You'll Learn Configure DNS using Bind 9 Set up Apache and Nginx Customize a mail server: IMAP (Dovecot) and SMTP (Postfix), spam filtering included Authenticate mail users using LDAP Install and maintain MariaDB and PostgreSQL databases Prepare SSL/TLS certificates for the encryption of web, mail and LDAP traffic Synchronize files, calendars and address books between devices Build a firewall: PF for FreeBSD and nftables for Linux Who This Book Is For This book can be used by aspiring and beginning system administrators who are working on personal servers, or more experienced system administrators who may know Unix well but need a reference book for the more specialized work that falls outside the daily routine. Basic understanding of Unix and working on the command line is necessary.

A practical and a fast paced guide that gives you all the information you need to make software development more cooperative and social. This book is written for team leaders and developers who wish to reap the benefit of Gerrit and improve collaboration by introducing code review practices.

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

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.

If you are looking for a low budget, small form-factor remotely accessible hacking tool, then the concepts in this book are ideal for you. If you are a penetration tester who wants to save on travel costs by placing a low-cost node on a target network, you will save thousands by using the methods covered in this book. You do not have to be a skilled hacker or programmer to use this book. It will be beneficial to have some networking experience; however, it is not required to follow the concepts covered in this book.

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

Interactive and Nonstandard Shell Features A Shell Summary B For More Information

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

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.

If you want to learn how to build efficient user interfaces with React, this is your book. Authors Alex Banks and Eve Porcello show you how to create UIs with this small JavaScript library that can deftly display data changes on large-scale, data-driven websites without page reloads. Along the way, you'll learn how to work with functional programming and the latest ECMAScript features. Developed by Facebook, and used by companies including Netflix, Walmart, and The New York Times for large parts of their web interfaces, React is quickly growing in use. By learning how to build React components with this hands-on guide, you'll fully understand how useful React can be in your organization. Learn key functional programming concepts with JavaScript Peek under the hood to understand how React runs in the browser Create application presentation layers by mounting and composing React components Use component trees to manage data and reduce the time you spend debugging applications Explore React's component lifecycle and use it to load data and improve UI performance Use a routing solution for browser history, bookmarks, and other features of single-page applications Learn how to structure React applications with servers in mind

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.

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.

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.

[Copyright: d0195a5064740716311f09c491e5dce0](https://www.d0195a5064740716311f09c491e5dce0)