

Ssh The Secure Shell The Definitive Guide

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

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

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

An easy to digest practical guide to Metasploit covering all aspects of the framework from installation, configuration, and vulnerability hunting to advanced client side attacks and anti-forensics. About This Book Carry out penetration testing in highly-secured environments with Metasploit Learn to bypass different defenses to gain access into different systems. A step-by-step guide that will quickly enhance your penetration testing skills. Who This Book Is For If you are a penetration tester, ethical hacker, or security consultant who wants to quickly learn the Metasploit framework to carry out elementary penetration testing in highly secured environments then, this book is for you. What You Will Learn Get to know the absolute basics of the Metasploit framework so you have a strong foundation for advanced attacks Integrate and use various supporting tools to make Metasploit even more powerful and precise Set up the Metasploit environment along with your own virtual testing lab Use Metasploit for information gathering and enumeration before planning the blueprint for the attack on the target system Get your hands dirty by firing up Metasploit in your own virtual lab and hunt down real vulnerabilities Discover the clever features of the Metasploit framework for launching sophisticated and deceptive client-side attacks that bypass the perimeter security Leverage Metasploit capabilities to perform Web application security scanning In Detail This book will begin by introducing you to Metasploit and its functionality. Next, you will learn how to set up and configure Metasploit on various platforms to create a virtual test environment. You will also get your hands on various tools and components used by Metasploit. Further on in the book, you will learn how to find weaknesses in the target system and hunt for vulnerabilities using Metasploit and its supporting tools. Next, you'll get hands-on experience carrying out client-side attacks. Moving on, you'll learn about web application security scanning and bypassing anti-virus and clearing traces on the target system post compromise. This book will also keep you updated with the latest security techniques and methods that can be directly applied to scan, test, hack, and secure networks and systems with Metasploit. By the end of this book, you'll get the hang of bypassing different defenses, after which you'll learn how hackers use the network to gain access into different systems. Style and approach This tutorial is packed with step-by-step instructions that are useful for those getting started with Metasploit. This is an easy-to-read guide to learning Metasploit from scratch that explains simply and clearly all you need to

know to use this essential IT power tool.

Using Samba

A Guide to Open Source Security

Security of Interactive and Automated Access Management Using Secure Shell (SSH)

Hack Proofing Linux

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

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.

This complete guide to setting up and running a TCP/IP network is essential for network administrators, and invaluable for users of home systems that access the Internet. The book starts with the fundamentals -- what protocols do and how they work, how addresses and routing are used to move data through the network, how to set up your network connection -- and then covers, in detail, everything you need to know to exchange information via the Internet. Included are discussions on advanced routing protocols (RIPv2, OSPF, and BGP) and the gated software package that implements them, a tutorial on configuring important network services -- including DNS, Apache, sendmail, Samba, PPP, and DHCP -- as well as expanded chapters on troubleshooting and security. TCP/IP Network Administration is also a command and syntax reference for important packages such as gated, pppd, named, dhcpd, and sendmail. With coverage that includes Linux, Solaris, BSD, and System V TCP/IP implementations, the third edition contains: Overview of TCP/IP Delivering the data Network services Getting started M Basic configuration Configuring the interface Configuring routing Configuring DNS Configuring network servers Configuring sendmail Configuring Apache Network security Troubleshooting Appendices include dip, pppd, and chat reference, a gated reference, a dhcpd reference, and a sendmail reference This new edition includes ways of configuring Samba to provide file and print sharing on networks that integrate Unix and Windows, and a new chapter is dedicated to the important task of configuring the Apache web server. Coverage of network security now includes details on OpenSSH, stunnel, gpg, iptables, and the access control mechanism in xinetd. Plus, the book offers updated information about DNS, including details on BIND 8 and BIND 9, the role of classless IP addressing and network prefixes, and the changing role of registrars. Without a doubt, TCP/IP Network Administration, 3rd Edition is a must-have for all network administrators and anyone who deals with a network that transmits data over the Internet.

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.

From Charles M. Kozierek, the creator of the highly regarded www.pcguides.com, comes The TCP/IP Guide. This completely up-to-date, encyclopedic reference on the TCP/IP protocol suite will appeal to newcomers and the seasoned professional alike. Kozierek details the core protocols that make TCP/IP internetworks function and the most important classic TCP/IP applications, integrating IPv6 coverage throughout. Over 350 illustrations and hundreds of tables help to explain the finer points of this complex topic. The book's personal, user-friendly writing style lets readers of all levels understand the dozens of protocols and technologies that run the Internet, with full coverage of PPP, ARP, IP, IPv6, IP NAT, IPSec, Mobile IP, ICMP, RIP, BGP, TCP, UDP, DNS, DHCP, SNMP, FTP, SMTP, NNTP, HTTP, Telnet, and much more. The TCP/IP Guide is a must-have addition to the libraries of internetworking students, educators, networking professionals, and those working toward certification.

SSH, the Secure Shell

Ssh The Secure Shell: The Definitive Guide

TCP/IP Network Administration

Secure your Linux server and protect it from intruders, malware attacks, and other external threats

LDAP System Administration

SSH, The Secure Shell

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.

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

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. 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.

Network Security Hacks

Implementing SSH

Mastering Unix Shell Scripting

A Comprehensive, Illustrated Internet Protocols Reference

Shell Programming in Unix, Linux and OS X

CentOS 8 Essentials

Arguably one of the most highly regarded and widely used enterprise level operating systems available today is the CentOS 8 distribution. Not only is it considered to be among the most stable and reliable operating systems, it is also backed by the considerable resources and technical skills of Red Hat, Inc. CentOS 8 Essentials is designed to provide detailed information on the

installation, use and administration of the CentOS 8 distribution. For beginners, the book covers topics such as operating system installation, the basics of the GNOME desktop environment, configuring email and web servers and installing packages and system updates using App Streams. Additional installation topics such as dual booting with Microsoft Windows are also covered, together with all important security topics such as configuring a firewall and user and group administration. For the experienced user, topics such as remote desktop access, the Cockpit web interface, logical volume management (LVM), disk partitioning, swap management, KVM virtualization, Secure Shell (SSH), Linux Containers and file sharing using both Samba and NFS are covered in detail to provide a thorough overview of this enterprise class operating system.

Original textbook (c) October 31, 2011 by Olivier Bonaventure, is licensed under a Creative Commons Attribution (CC BY) license made possible by funding from The Saylor Foundation's Open Textbook Challenge in order to be incorporated into Saylor's collection of open courses available at: <http://www.saylor.org>. Free PDF 282 pages at <https://www.textbookequity.org/bonaventure-computer-networking-principles-protocols-and-practice/> This open textbook aims to fill the gap between the open-source implementations and the open-source network specifications by providing a detailed but pedagogical description of the key principles that guide the operation of the Internet. 1 Preface 2 Introduction 3 The application Layer 4 The transport layer 5 The network layer 6 The datalink layer and the Local Area Networks 7 Glossary 8 Bibliography

This book is a comprehensive guide to utilizing and creating Ruby Gems.

Coverage provides an enormous code library that will help developers improve their projects. It details 34 of the best and most useful Gems, including ones to speed up web applications, process credit card payments, produce PDF documents, read and update RSS feeds, and acquire real-time shipping prices from FedEx and UPS. Each of these also comes complete with actual use cases and code examples that readers can immediately use in their own projects. In addition, the book describes how readers can package and distribute their own Ruby Gems.

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.

Strategies for Optimizing the Secure Shell

Network Security with OpenSSL

The TCP/IP Guide

A File & Print Server for Linux, Unix & Mac OS X

SSH, The Secure Shell: The Definitive Guide

BeagleBone For Dummies

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

FRIGHTENED MONSTERS. STOLEN TIME. AND ONE SERIOUSLY UNDERESTIMATED DAMSEL. Katie ran from the magical world years ago. She never planned on being dragged back in by a prophesying clamshell. The seers believe she alone can prevent an apocalypse of ruined time and broken worlds. Bran the Crow King believes she can save him from his cannibalistic grandfather. Katie believes they're all nuts. One thing is for certain: she's not waiting around for help. Operation Katie Saves her Own Damn Self

is officially on.

"Get the most from cPanel with this easy to follow guide."--Resource description p.

The best-selling text on SSH, newly revised and updated! Secure Shell (SSH) lets sysadmins securely manage remote systems. It's powerful, complicated, and confusing. Lose the confusion. SSH Mastery: OpenSSH, PuTTY, Tunnels and Keys rescues you from sifting through decades of obsolete online tutorials and quickly makes you an SSH journeyman. You'll learn to · eliminate passwords · manage access by users, groups, addresses, and more · securely move files around your network · forward graphic displays · proxy TCP connections · build SOCKS proxies · centrally manage and distribute keys and configurations · use SSH as secure transport for other applications · build virtual private networks · create Certificate Authorities for truly large scale deployment Master Secure Shell with SSH Mastery!

#ssh2e

Security Tools & Techniques

SSH, The Secure Shell. The Definitive Guide

Learning Python Networking

SSH Mastery

CPanel User Guide and Tutorial

The Linux Enterprise Cluster

A comprehensive guide to penetration testing cloud services deployed with Microsoft Azure, the cloud computing service provider used by companies like Warner Brothers and Apple. Pentesting Applications is a comprehensive guide to penetration testing cloud services deployed in Microsoft Azure, the popular cloud computing service provider used by numerous companies. You'll start learning how to approach a cloud-focused penetration test and how to obtain the proper permissions to execute it; then, you'll learn to perform reconnaissance on an Azure subscription, gain access to Storage accounts, and dig into Azure's Infrastructure as a Service (IaaS). You'll also learn how to uncover weaknesses in virtual machine settings that enable you to acquire passwords, binaries, and settings files - Use PowerShell commands to find IP addresses, administrative users, and network details - Find security issues related to multi-factor authentication and management certificates - Penetrate networks by enumerating firewall rules - Investigate specialized services like Azure Key Vault, Azure Web Apps, and Azure Automation - View logs and security events to find out when you've been caught Packed with sample pentesting scripts, practical advice for completing security assessments, and tips that explain how companies can configure Azure to foil common attacks, Pentesting Azure Applications is a clear overview of how to effectively perform cloud-focused security tests and report accurate findings and recommendations.

Shell Programming in Unix, Linux and OS X is a thoroughly updated revision of Kochan and Woodcock'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 in 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 t

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 your shell environment Make use of functions Debug scripts Contents at a Glance 1 A Quick Review of Shell 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 Interactions with Nonstandard Shell Features A Shell Summary B For More Information

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 share 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 a 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, platform compatibility, and resource discovery that make the difference between whether users find the folder they expect or a cryptic error message. The current edition covers such advanced features as Integration with Active Directory and OpenLDAP Migrating from Windows NT 4.0 domains to Samba 4 Delegating administrative tasks to non-root users Central printer management Advanced file sharing features, such as making use of Virtual File System (VFS) plugins. Samba is a cross-platform tool that is 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 and in Samba itself. Whether you're playing on your personal computer or an enterprise network, this book is a note or a full three-octave range, Using Samba will give you an efficient and secure server.

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 work 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 (LVS) load balancing software, how to configure a reliable printing system in a Linux cluster environment, 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 useful for System Administrators even if they are not building a cluster. Anyone interested in deploying Samba 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.

Using Secure Shell (SSH) to Improve Router Security
Build a Highly Available Cluster with Commodity Hardware and Free Software
Pentesting Azure Applications

A complete guide to build and deploy strong networking capabilities using Python 3.7 and Ansible 2.7 Edition

The Definitive Guide to Testing and Securing Deployments

Unix Power Tools

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.

* 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.

CD-ROM includes: Implementations of Secure Shell for UNIX, Windows, and other operating systems; SecureCRT; F-Secure SSH Windows clients; NT port for ssh and sshd clients; VMS client; F-Secure SSH Macintosh clients.

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

Git Pocket Guide

Computer Networking

Learn to Build a Fully Functional and Well-Secured Enterprise Class Internet Server

Pro OpenSSH

PfSense 2 Cookbook

Help for Unix System Administrators

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

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.

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.

Achieve improved network programmability and automation by leveraging powerful network programming concepts, algorithms, and tools
Key Features
Deal with remote network servers using SSH, FTP, SNMP and LDAP protocols. Design multi threaded and event-driven architectures for asynchronous servers programming. Leverage your Python programming skills to build powerful network applications
Book Description
Network programming has always been a demanding task. With full-featured and well-documented libraries all the way up the stack, Python makes network programming the enjoyable experience it should be. Starting with a walk through of today's major networking protocols, through this book, you'll learn how to employ Python for network programming, how to request and retrieve web resources, and how to extract data in major formats over the web. You will utilize Python for emailing using different protocols, and you'll interact with remote systems and IP and DNS networking. You will cover the connection of networking devices and configuration using Python 3.7, along with cloud-based network management tasks using Python. As the book progresses, socket programming will be covered, followed by how to design servers, and the pros and cons of multithreaded and event-driven architectures. You'll develop practical clientside applications, including web API clients, email clients, SSH, and FTP. These applications will also be implemented through existing web application frameworks. What you will learn
Execute Python modules on networking tools
Automate tasks regarding the analysis and extraction of information from a network
Get to grips with asynchronous programming modules available in Python
Get to grips with IP address manipulation modules using Python programming
Understand the main frameworks available in Python that are focused on web application
Manipulate IP addresses and perform CIDR calculations
Who this book is for
If you're a Python developer or a system administrator with Python experience and you're looking to take your first steps in network programming, then this book is for you. If you're a network engineer or a network professional aiming to be more productive and efficient in networking programmability and automation then this book would serve as a useful resource. Basic knowledge of Python is assumed.

The Fourth Edition of Unix Shell Programming

Metasploit for Beginners

A Working Introduction

Cryptography for Secure Communications

The Definitive Guide

Linux Pocket Guide

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.

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.

Secure Shell (SSH) lets systems administrators securely manage remote systems. But most people only use the bare minimum SSH offers. Used properly, SSH simplifies your job. This book saves you from sifting a decade of obsolete online tutorials and quickly gets you running: SSH with the OpenSSH server and the PuTTY and OpenSSH clients. You will: Eliminate passwords. Manage access to your SSH server by users, groups, addresses, and more Securely move files around your network Forward graphic displays from one host to another Forward TCP connections Centrally manage host keys and client configurations Use SSH as a secure transport for other applications Secure applications run over SSH Build Virtual Private Networks with OpenSSH And more! This book simplifies the work of anyone using SSH. Small enough to read and implement quickly, exhaustive enough to include everything most of us need plus a little more.

Master SSH with SSH Mastery

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.

Unix Secure Shell

OpenSSH, PuTTY, Tunnels, and Keys

Mastering Linux Security and Hardening

Putting Directories to Work

Secure Shell in the Enterprise

Practical Ruby Gems