Linux Firewalls Enhancing Security With Nftables And Beyond 4th Edition

Know Your Network
Pro Linux System Administration
Red Hat Linux Firewalls
Building Internet Firewalls
Mastering Linux Administration
Mastering Linux Security and Hardening
Enhancing Security with Nftables and Beyond
Help for Network Administrators
Network Security Hacks
From Asterisk to Zebra with Easy-to-Use Recipes
Building Secure Servers with Linux
Practical UNIX and Internet Security
A Hacker's Guide to Protecting Your Linux Server and Workstation
Linux Network Administrator's Guide
Maximum Linux Security
Linux Security Fundamentals
A Guide to Open Source Security
Firewalls, NAT & Accounting
Attack Detection and Response with iptables, psad, and fwsnort
The Best Damn Firewall Book Period

Beginning Ethical Hacking with Kali Linux
A comprehensive guide to installing, configuring, and maintaining Linux systems in the modern data center
Linux Networking Cookbook
Mastering Linux Security and Hardening
Enhancing Security with nftables and Beyond
Building DMZs For Enterprise Networks
Linux iptables Pocket Reference
Linux Networking Cookbook
Computer and Network Security Essentials
Server Security from TLS to Tor
The Best Damn Firewall Book Period
Guidelines on Firewalls and Firewall Policy
Secure your Linux server and protect it from intruders, malware attacks, and other external threats
Linux Firewalls
Linux Firewalls
Network Security Assessment
Firewalls For Dummies
Linux Hardening in Hostile Networks
Red Hat Linux Security and Optimization

MCCULLOUGH HOLMES

Know Your Network *Red Hat What an amazing world we live in! Almost anything you can imaginecan be researched, compared, admired, studied, and in many cases,bought, with the click

of a mouse. The Internet has changed ourlives, putting a world of opportunity before us. Unfortunately, ithas also put a world of opportunity into the hands of those whosemotives are less than honorable. A firewall, a piece of software orhardware that erects a barrier between your computer and those whomight like to invade it, is one solution. If you've been using the Internet for any length of time,you've probably received some unsavory and unsolicitede-mail. If you run a business, you may be worried about thesecurity of your data and your customers' privacy. At home,you want to protect your personal information from identity thievesand other shady characters. Firewalls ForDummies® will give you the lowdown onfirewalls, then guide you through choosing, installing, andconfigurin g one for your personal or bus iness network. Firewalls For Dummies® helps youunderstan d what firewalls are, how they operate on different typesof networks, what they can and can't do, and how to pick agood one (it's easier than identifying that perfect melon inthe supermarket.) You'll find out about Developing security

policies Establishing rules for simple protocols Detecting and responding to system intrusions Setting up firewalls for SOHO or personal use Creating demilitarized zones Using Windows or Linux as a firewall Configuring ZoneAlarm, BlackICE, and Norton personalfirewalls Installing and using ISA server and FireWall-1 With the handy tips and hints this book provides, you'llfind that firewalls are nothing to fear – that is,unless you're a cyber-crook! You'll soon be able tokeep your data safer, protect your family's privacy, andprobably sleep better, too.

Pro Linux System Administration Sams Publishing This introduction to networking on Linux now covers firewalls, including the use of ipchains and Netfilter, masquerading , and accounting. Other new topics in this second edition include Novell (NCP/IPX) support and INN (news administration).

Addison-Wesley Professional This soup-to-nuts collection of recipes covers everything you need to know to perform your job as a Linux network administrator, whether you're new to the job or have years of experience. With Linux Networking

Cookbook, you'll dive straight into the gnarly hands-on work of building and maintaining a computer network. Running a network doesn't mean you have all the answers. Networking is a complex subject with reams of reference material that's difficult to keep straight, much less remember. If you want a book that lays out the steps for specific tasks, that clearly explains the commands and configurations , and does not tax your patience with endless ramblings and meanderings into theory and obscure RFCs, this is the book for you. You will find recipes for: Building a gateway, firewall, and wireless access point on a Linux network Building a VoIP server with Asterisk Secure remote administration with SSH Building secure VPNs with OpenVPN, and a Linux PPTP VPN server Single sign-on with Samba for mixed Linux/Windows LANs Centralized network directory with OpenLDAP Network monitoring with Nagios or MRTG Getting acquainted with IPv6 Setting up hands-free networks installations of new systems Linux system administration via serial console And a lot more. Each recipe includes a clear, hands-on solution with tested

code, plus a discussion on why it works. When you need to solve a network problem without delay, and don't have the time or patience to comb through reference books or the Web for answers, Linux Networking Cookbook gives you exactly what you need. **Red Hat Linux Firewalls** "O'Reilly Media, Inc." Over 40 recipes to help you set up and configure Linux networks About This Book Move beyond the basics of how a Linux machine works and gain a better understanding of Linux networks and their configuration Impress your peers by setting up and configuring a Linux server and its various network elements like a pro This is a hands-on solution guide to building, maintaining, and securing a network using Linux Who This Book Is For This book is targeted at Linux systems administrators who have a good basic understanding and some prior experience of how a Linux machine operates, but want to better understand how various network services function, how to set them up, and how to secure them. You should be familiar with how to set up a Linux server and how to install additional software on them. What You Will Learn

Route an IPv6 netblock to your local network Modify your named instance to support setting hostnames for your IPv6 addresses Use SSH for remote console access Configure NGINX with TLS Secure XMPP with TLS Leverage iptables6 to firewall your IPv6 traffic Configure Samba as an Active Directory compatible directory service In Detail Linux can be configured as a networked workstation, a DNS server, a mail server, a firewall, a gateway router, and many other things. These are all part of administration tasks, hence network administration is one of the main tasks of Linux system administration . By knowing how to configure system network interfaces in a reliable and optimal manner, Linux administrators can deploy and configure several network services including file, web, mail, and servers while working in large enterprise environments. Starting with a simple Linux router that passes traffic between two private networks, you will see how to enable NAT on the router in order to allow Internet access from the network, and will also enable DHCP on the network to ease configuration of client systems. You

will then move on to configuring your own DNS server on your local network using bind9 and tying it into your DHCP server to allow automatic configuration of local hostnames. You will then future enable your network by setting up IPv6 via tunnel providers. Moving on, we'll configure Samba to centralize authentication for your network services; we will also configure Linux client to leverage it for authentication , and set up a RADIUS server that uses the directory server for authentication . Toward the end, you will have a network with a number of services running on it, and will implement monitoring in order to detect problems as they occur. Style and approach This book is packed with practical recipes and a task-based approach that will walk you through building, maintaining, and securing a computer network using Linux.

Building Internet Firewalls

Packt Publishing Ltd

This book is essential reading for anyone wanting to protect Internet-connected computers from unauthorized access. Coverage includes TCP/IP, setting up firewalls, testing and maintaining firewalls, and much more. All of the

major important firewall products are covered including Microsoft Internet Security and Acceleration Server (ISA), ISS BlackICE, Symantec Firewall, Check Point NG, and PIX Firewall. Firewall configuration strategies and techniques are covered in depth. The book answers questions about firewalls, from How do I make Web/HTTP work through my firewall? To What is a DMZ, and why do I want one? And What are some common attacks, and how can I protect my system against them? The Internet's explosive growth over the last decade has forced IT professionals to work even harder to secure the private networks connected to it—from erecting firewalls that keep out malicious intruders to building virtual private networks (VPNs) that permit protected, fully encrypted communications over the Internet's vulnerable public infrastructure. The Best Damn Firewalls Book Period covers the most popular Firewall products, from Cisco's PIX Firewall to Microsoft's ISA Server to CheckPoint NG, and all the components of an effective firewall set up. Anything needed to protect the

perimeter of a network can be found in this book. - This book is all encompassing , covering general Firewall issues and protocols, as well as specific products. - Anyone studying for a security specific certification, such as SANS' GIAC Certified Firewall Analyst (GCFW) will find this book an invaluable resource. - The only book to cover all major firewall products from A to Z: CheckPoint, ISA Server, Symatec, BlackICE, PIX Firewall and Nokia.

Mastering Linux Administration Addison-Wesley Professional

As a network administrator, auditor or architect, you know the importance of securing your network and finding security solutions you can implement quickly. This succinct book departs from other security literature by focusing exclusively on ways to secure Cisco routers, rather than the entire network. The rational is simple: If the router protecting a network is exposed to hackers, then so is the network behind it. Hardening Cisco Routers is a reference for protecting the protectors. Included are the following topics: The importance of router security and where routers fit into an overall security plan Different router configurations

for various versions of Cisco?s IOS Standard ways to access a Cisco router and the security implications of each Password and privilege levels in Cisco routers Authentication , Authorization, and Accounting (AAA) control Router warning banner use (as recommended by the FBI) Unnecessary protocols and services commonly run on Cisco routers SNMP security Anti-spoofing Protocol security for RIP, OSPF, EIGRP, NTP, and BGP Logging violations Incident response Physical security Written by Thomas Akin, an experienced Certified Information Systems Security Professional (CISSP) and Certified Cisco Academic Instructor (CCAI), the book is well organized, emphasizing practicality and a hands-on approach. At the end of each chapter, Akin includes a Checklist that summarizes the hardening techniques discussed in the chapter. The Checklists help you double-check the configurations you have been instructed to make, and serve as quick references for future security procedures.Concise and to the point, Hardening Cisco Routers supplies you with all the tools necessary to turn a

potential vulnerability into a strength. In an area that is otherwise poorly documented, this is the one book that will help you make your Cisco routers rock solid.
Mastering Linux Security and Hardening
Elsevier
Learn how to secure your system and implement QoS using real-world scenarios for networks of all sizes.
Enhancing Security with Nftables and Beyond
Elsevier
Get started in white-hat ethical hacking using Kali Linux. This book starts off by giving you an overview of security trends, where you will learn the OSI security architecture. This will form the foundation for the rest of Beginning Ethical Hacking with Kali Linux. With the theory out of the way, you'll move on to an introduction to VirtualBox, networking, and common Linux commands, followed by the step-by-step procedure to build your own web server and acquire the skill to be anonymous . When you have finished the examples in the first part of your book, you will have all you need to carry out safe and ethical hacking experiments. After an introduction to Kali Linux, you will carry out your first penetration tests with Python and code raw binary packets for use in

those tests. You will learn how to find secret directories on a target system, use a TCP client in Python, and scan ports using NMAP. Along the way you will discover effective ways to collect important information, track email, and use important tools such as DMITRY and Maltego, as well as take a look at the five phases of penetration testing. The coverage of vulnerability analysis includes sniffing and spoofing, why ARP poisoning is a threat, how SniffJoke prevents poisoning, how to analyze protocols with Wireshark, and using sniffing packets with Scapy. The next part of the book shows you detecting SQL injection vulnerabilities, using sqlmap, and applying brute force or password attacks. Besides learning these tools, you will see how to use OpenVas, Nikto, Vega, and Burp Suite. The book will explain the information assurance model and the hacking framework Metasploit, taking you through important commands, exploit and payload basics. Moving on to hashes and passwords you will learn password testing and hacking techniques with John the Ripper and Rainbow. You will then dive into classic and modern

encryption techniques where you will learn the conventional cryptosystem. In the final chapter you will acquire the skill of exploiting remote Windows and Linux systems and you will learn how to own a target completely. What You Will Learn Master common Linux commands and networking techniques Build your own Kali web server and learn to be anonymous Carry out penetration testing using Python Detect sniffing attacks and SQL injection vulnerabilities Learn tools such as SniffJoke, Wireshark, Scapy, sqlmap, OpenVas, Nikto, and Burp Suite Use Metasploit with Kali Linux Exploit remote Windows and Linux systems Who This Book Is For Developers new to ethical hacking with a basic understanding of Linux programming. *Help for Network Administrators* "O'Reilly Media, Inc." PART OF THE NEW JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES Fully revised and updated with the latest data from the field, Network Security, Firewalls, and VPNs, Second Edition provides a unique, in-depth look at the major business challenges and threats that are introduced when an organization s network is

connected to the public Internet. Written by an industry expert, this book provides a comprehensive explanation of network security basics, including how hackers access online networks and the use of Firewalls and VPNs to provide security countermeasures. Using examples and exercises, this book incorporates hands-on activities to prepare the reader to disarm threats and prepare for emerging technologies and future attacks. Key Features: - Introduces the basics of network security exploring the details of firewall security and how VPNs operate - Illustrates how to plan proper network security to combat hackers and outside threats - Discusses firewall configuration and deployment and managing firewall security - Identifies how to secure local and internet communications with a VPN Instructor Materials for Network Security, Firewalls, VPNs include: PowerPoint Lecture Slides Exam Questions Case Scenarios/Handouts About the Series This book is part of the Information Systems Security and Assurance Series from Jones and Bartlett Learning. Designed for courses and

curriculums in IT Security, Cybersecurity, Information Assurance, and Information Systems Security, this series features a comprehensive, consistent treatment of the most current thinking and trends in this critical subject area. These titles deliver fundamental information-security principles packed with real-world applications and examples. Authored by Certified Information Systems Security Professionals (CISSPs), they deliver comprehensive information on all aspects of information security. Reviewed word for word by leading technical experts in the field, these books are not just current, but forward-thinking putting you in the position to solve the cybersecurity challenges not just of today, but of tomorrow, as well."

Network Security Hacks Packt Publishing Ltd

"The Second Edition of Security Strategies in Linux Platforms and Applications opens with a discussion of risks, threats, and vulnerabilities. Part 2 discusses how to take advantage of the layers of security and the modules associated with AppArmor and SELinux. Part 3 looks at the use of open source and proprietary tools when building a layered security

strategy"-- *From Asterisk to Zebra with Easy-to-Use Recipes* Apress Introduces the authors' philosophy of Internet security, explores possible attacks on hosts and networks, discusses firewalls and virtual private networks, and analyzes the state of communicatio n security. Building Secure Servers with Linux DIANE Publishing Earlier ed. authored by Robert L. Ziegler. **Practical UNIX and Internet Security** John Wiley & Sons Details all the Linux system holes, attack methods, and hacker's tools that hackers have had years to study, explore, and improve upon, helping Linux administrators identify and plug security holes on their systems. Original. (Intermediate/ Advanced). *A Hacker's Guide to Protecting Your Linux Server and Workstation* Pearson Education Addressing the firewall capabilities of Linux, a handbook for security professionals describes the Netfilter infrastruction 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)

Linux Network Administrator's Guide

Sams Publishing

Rely on this practical, end-to-end guide on cyber safety and online security written expressly for a non-technical audience. You will have just what you need to protect yourself—step by step, without judgment, and with as little jargon as possible. Just how secure is your computer right now? You probably don't really know. Computers and the Internet have revolutionized the modern world, but if you're like most people, you have no clue how these things work and don't know the real threats. Protecting your computer is like defending a medieval castle. While moats, walls, drawbridges, and castle guards can be effective, you'd go broke trying to build something dragon-proof. This book is not about protecting yourself from a targeted attack by the NSA; it's about armoring yourself against common hackers and mass surveillance. There are dozens of no-brainer things we all should be doing to protect our computers and safeguard our data—just like wearing a seat belt, installing smoke alarms, and putting on

sunscreen. Author Carey Parker has structured this book to give you maximum benefit with minimum effort. If you just want to know what to do, every chapter has a complete checklist with step-by-step instructions and pictures. The book contains more than 150 tips to make you and your family safer. It includes: Added steps for Windows 10 (Spring 2018) and Mac OS X High Sierra Expanded coverage on mobile device safety Expanded coverage on safety for kids online More than 150 tips with complete step-by-step instructions and pictures What You'll Learn Solve your password problems once and for all Browse the web safely and with confidence Block online tracking and dangerous ads Choose the right antivirus software for you Send files and messages securely Set up secure home networking Conduct secure shopping and banking online Lock down social media accounts Create automated backups of all your devices Manage your home computers Use your smartphone and tablet safely Safeguard your kids online And more! Who This Book Is For Those who use computers and mobile devices, but don't really know (or frankly care) how they

work. This book is for people who just want to know what they need to do to protect themselves—step by step, without judgment, and with as little jargon as possible. *Maximum Linux Security* Elsevier When Practical Unix Security was first published more than a decade ago, it became an instant classic. Crammed with information about host security, it saved many a Unix system administrator from disaster. The second edition added much-needed Internet security coverage and doubled the size of the original volume. The third edition is a comprehensive update of this very popular book - a companion for the Unix/Linux system administrator who needs to secure his or her organization's system, networks, and web presence in an increasingly hostile world.Focusing on the four most popular Unix variants today--Solaris, Mac OS X, Linux, and FreeBSD--this book contains new information on PAM (Pluggable Authentication Modules), LDAP, SMB/Samba, anti-theft technologies, embedded systems, wireless and laptop issues, forensics, intrusion detection, chroot jails, telephone scanners and firewalls, virtual and cryptographic

filesystems, WebNFS, kernel security levels, outsourcing, legal issues, new Internet protocols and cryptographic algorithms, and much more.Practical Unix & Internet Security consists of six parts: Computer security basics: introduction to security problems and solutions, Unix history and lineage, and the importance of security policies as a basic element of system security. Security building blocks: fundamentals of Unix passwords, users, groups, the Unix filesystem, cryptography, physical security, and personnel security. Network security: a detailed look at modem and dialup security, TCP/IP, securing individual network services, Sun's RPC, various host and network authentication systems (e.g., NIS, NIS+, and Kerberos), NFS and other filesystems, and the importance of secure programming. Secure operations: keeping up to date in today's changing security world, backups, defending against attacks, performing integrity management, and auditing. Handling security incidents: discovering a break-in, dealing with programmed threats and denial of service attacks, and

legal aspects of computer security. Appendixes: a comprehensive security checklist and a detailed bibliography of paper and electronic references for further reading and research. Packed with 1000 pages of helpful text, scripts, checklists, tips, and warnings, this third edition remains the definitive reference for Unix administrators and anyone who cares about protecting their systems and data from today's threats. **Linux Security Fundamentals** "O'Reilly Media, Inc." Implement Industrial-Strength Security on Any Linux Server In an age of mass surveillance, when advanced cyberwarfare weapons rapidly migrate into every hacker’s toolkit, you can’t rely on outdated security methods–especially if you’re responsible for Internet-facing services. In Linux® Hardening in Hostile Networks, Kyle Rankin helps you to implement modern safeguards that provide maximum impact with minimum effort and to strip away old techniques that are no longer worth your time. Rankin provides clear, concise guidance on modern workstation, server, and network hardening, and explains how to harden specific

services, such as web servers, email, DNS, and databases. Along the way, he demystifies technologies once viewed as too complex or mysterious but now essential to mainstream Linux security. He also includes a full chapter on effective incident response that both DevOps and SecOps can use to write their own incident response plan. Each chapter begins with techniques any sysadmin can use quickly to protect against entry-level hackers and presents intermediate and advanced techniques to safeguard against sophisticated and knowledgeable attackers, perhaps even state actors. Throughout, you learn what each technique does, how it works, what it does and doesn't protect against, and whether it would be useful in your environment. Apply core security techniques including 2FA and strong passwords Protect admin workstations via lock screens, disk encryption, BIOS passwords, and other methods Use the security-focused Tails distribution as a quick path to a hardened workstation Compartmentalize workstation tasks into VMs with varying levels of trust Harden servers with SSH, use apparmor and sudo to limit

the damage attackers can do, and set up remote syslog servers to track their actions
Establish secure VPNs with OpenVPN, and leverage SSH to tunnel traffic when VPNs can't be used
Configure a software load balancer to terminate SSL/TLS connections and initiate new ones downstream
Set up standalone Tor services and hidden Tor services and relays
Secure Apache and Nginx web servers, and take full advantage of HTTPS
Perform advanced web server hardening with HTTPS forward secrecy and ModSecurity web application firewalls
Strengthen email security with SMTP relay authentication, SMTPS, SPF records, DKIM, and DMARC
Harden DNS servers, deter their use in DDoS attacks, and fully implement DNSSEC
Systematically protect databases via network access control, TLS traffic encryption, and encrypted data storage
Respond to a compromised server, collect evidence, and prevent future attacks
Register your product at informit.com/register for convenient access to downloads, updates, and corrections as they become available.

A Guide to Open Source Security
Apress
This updated

report provides an overview of firewall technology, and helps organizations plan for and implement effective firewalls. It explains the technical features of firewalls, the types of firewalls that are available for implementation by organizations, and their security capabilities. Organizations are advised on the placement of firewalls within the network architecture, and on the selection, implementation, testing, and management of firewalls. Other issues covered in detail are the development of firewall policies, and recommendations on the types of network traffic that should be prohibited. The appendices contain helpful supporting material, including a glossary and lists of acronyms and abreviations; and listings of in-print and online resources. Illus.

Firewalls, NAT & Accounting

Elsevier

This book covers what an administrator needs to plan out and integrate a DMZ into a network for small, medium and Enterprise networks. In most enterprises the perception is that a firewall provides a hardened perimeter. However, the security of internal networks and hosts is usually very soft. In such

an environment, a non-DMZ system that is offering services to the Internet creates the opportunity to leapfrog to other hosts in the soft interior of your network. In this scenario your internal network is fair game for any attacker who manages to penetrate your so-called hard perimeter. - There are currently no books written specifically on DMZs - This book will be unique in that it will be the only book that teaches readers how to build a DMZ using all of these products: ISA Server, Check Point NG, Cisco Routers, Sun Servers, and Nokia Security Appliances. - Dr. Thomas W. Shinder is the author of the best-selling book on Microsoft's ISA, Configuring ISA Server 2000. Customers of the first book will certainly buy this book. *Attack Detection and Response with iptables, psad, and fwsnort* *Red Hat * Everything readers need to construct firewalls that protect computer networks from attacks and intrusions * Covers the migration from ipchains and how to mange iptable log files * Reviews the customization of firewalls, the Red Hat firewall tool, the firewall setup, and advanced firewall features * Includes numerous examples of firewalls and

firewall administration techniques that work on Red Hat Linux systems * Explains how to cost-justify, implement, test, and operate packet filtering firewalls constructed using Red Hat Linux RED HAT(r) PRESS(TM) Linux Solutions from the Experts at Red Hat Red Hat-the world's leading Linux company-presents a series of unrivaled guides that are reviewed and approved by the experts at Red Hat. Each book is packed with invaluable tips and techniques that are ideal for everyone from beginning to advanced network and systems professionals, as well as home and small businesses.

Do Not!
• The Wonderful Things You Will Be By Emily Winfield Martin
• Can't Hurt Me: Master Your Mind And Defy The Odds
• Fast Like A Girl: A Woman's Guide To Using The Healing Power Of Fasting To Burn Fat, Boost Energy, And Balance Hormones