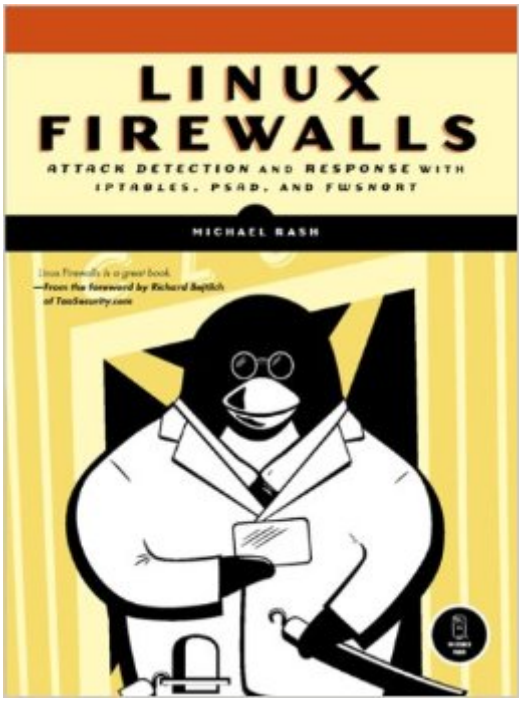
Linux Firewalls: Attack Detection And Response



Synopsis

System administrators need to stay ahead of new security vulnerabilities that leave their networks exposed every day. A firewall and an intrusion detection systems (IDS) are two important weapons in that fight, enabling you to proactively deny access and monitor network traffic for signs of an attack.Linux Firewalls discusses the technical details of the iptables firewall and the Netfilter framework that are built into the Linux kernel, and it explains how they provide strong filtering, Network Address Translation (NAT), state tracking, and application layer inspection capabilities that rival many commercial tools. You'll learn how to deploy iptables as an IDS with psad and fwsnort and how to build a strong, passive authentication layer around iptables with fwknop.Concrete examples illustrate concepts such as firewall log analysis and policies, passive network authentication and authorization, exploit packet traces, Snort ruleset emulation, and more with coverage of these topics: Passive network authentication and OS fingerprintingiptables log analysis and policiesApplication layer attack detection with the iptables string match extensionBuilding an iptables ruleset that emulates a Snort rulesetPort knocking vs. Single Packet Authorization (SPA)Tools for visualizing iptables logsPerl and C code snippets offer practical examples that will help you to maximize your deployment of Linux firewalls. If you're responsible for keeping a network secure, you'll find Linux Firewalls invaluable in your attempt to understand attacks and use iptables-along with psad and fwsnort-to detect and even prevent compromises.

Book Information

File Size: 1723 KB

Print Length: 336 pages

Simultaneous Device Usage: Unlimited

Publisher: No Starch Press; 1 edition (September 24, 2007)

Publication Date: August 20, 2009

Sold by:Â Digital Services LLC

Language: English

ASIN: B002N3M6S6

Text-to-Speech: Enabled

X-Ray: Not Enabled

Word Wise: Not Enabled

Lending: Not Enabled

Enhanced Typesetting: Not Enabled

Best Sellers Rank: #212,119 Paid in Kindle Store (See Top 100 Paid in Kindle Store) #69 inÂ Books > Computers & Technology > Operating Systems > Linux > Programming #77 inÂ Books > Computers & Technology > Operating Systems > Linux > Networking & System Administration #157 inÂ Books > Computers & Technology > Security & Encryption > Privacy & Online Safety

Customer Reviews

Make no mistake, this book is on what it says it’s about "Attack Detection and Response with iptables, psad, and fwsnort" it contains very little information about setting up iptables to block unwanted external traffic.HOWEVER setting up iptables (in the basic sense) doesn’t require an entire book. Sure there are whole books on that topic but there is no need for a 300 page book on it, that just seems to be the size computer books have to be in order to get published. Which means other books on iptables are probably going to about 250 pages of fluff.Incidentally this book actually only spends about the first 35 pages describing that, the remainder is fantastic, useful, well written information about doing the things that make iptables truly useful. "detection and response" ACTIVELY securing your system.In addition to being comprehensive and useful this book happens to be well written, far better than most technical books.If you’re thinking about buying a book on Linux firewalls, make it this one, but if you’re not already familiar with iptables expect to read the first 35 pages, then a couple online tutorials and then come back to this book.

When I bought "Linux Firewalls" I was expecting a good book because I already knew that the work of Michael Rash is excellent. However, I expected the traditional Iptables handbook that looks more like a "man page". Surprisingly I found that the book was much better than that. Instead of detailing every single feature of the Iptables infrastructure, Michael Rash explains how Iptables can be used as a powerful (and free) Intrusion Detection/Prevention System. To achieve that, Rash presents three open source tools developed by himself: psad, an iptables-based port scan detector, fwsnort, a tool that translates snort rules into iptables sentences, and fwknop, a Port Knocking and SPA authentication system.The book is very practical. It’s amazing how everything is presented so clearly and with such useful examples. The author first introduces the potential threats that are associated with the Network Layer, Transport Layer and Application Layer (I loved those chapters). Then he starts discussing the detection of malicious attackers that try to break into the system. Finally he presents active response mechanisms against attackers and ways to secure the whole system with additional layers of security.The book is great if what you want is to secure your Linux

system using IPtables and the open source tools developed by Rash. Rash is an expert on firewalls and intrusion detection systems. If you follow his suggestions you'll build a very secure system. Firewall enthusiasts and TCP/IP fans will also enjoy reading the book because its written by a geek and its written for geeks. However, if you are looking for an Iptables handbook, you are looking for a theoretical book about Firewalls or you want to use other tools than the ones presented in the book, then "Linux Firewalls" may not be the best option for you.

Disclaimer: I wrote the foreword for this book, so obviously I am biased. However, I am not financially compensated for this book's success.In the foreword I note that Linux Firewalls is a "great book." As a FreeBSD user, Linux Firewalls is good enough to make me consider using Linux in certain circumstances! Mike's book is exceptionally clear, organized, concise, and actionable. You should be able to read it and implement everything you find by following his examples. You will not only learn tools and techniques, but you will be able to appreciate Mike's keen defensive insights.The majority of the world's digital security professionals focus on defense, because offense is left to the bad guys, police, and military. I welcome books like Linux Firewalls that bring real defensive tools and techniques to the masses in a form that can be digested and deployed for minimum cost and effort.One of the main reasons Linux Firewalls is a great book is that Mike Rash is an excellent writer. I've read (or tried to read) plenty of books that seemed to offer helpful content, but the author had no clue how to deliver that content in a readable manner. Linux Firewalls makes learning network security an enjoyable experience. Mike is exceptionally detail-oriented (see the RST vs RST ACK issue on p 63 and elsewhere) and he often cites sources and additional references. Linux Firewalls very nicely integrates sample network traffic to make numerous points; Ch 11 has several great examples. The sections on Fwsnort even improved my understanding of Snort itself.The bottom line is that if you are a user of non-Microsoft operating systems (Linux, BSD, etc.) and you want to know how Linux can help defend your network, you will enjoy reading Linux Firewalls.

Length: 2:41 Mins

Not for beginners, you need some tech background to get much out of this.(Full text review at [...])

Who needs a specialist distro or Vyatta? Get this book and you'll be up and running in no time. I thought the content was presented in a logical manner, concise, clear and very informative. From

IPTables novice to expert, there is a lot of good information in this book. If you want to understand the inner-workings of firewall based distros or products like Vyatta - or Brocade, whatever they call themselves these days - this is a good start. It introduces IPS/IDS basics, how to configure adaptive firewalls, and following the examples you will have the ability to set up a good, secure firewall in no time. I certainly recommend this book to anyone looking to get into the security field as well.

Linux Firewalls: Attack Detection and Response LINUX: Linux Command Line, Cover all essential Linux commands. A complete introduction to Linux Operating System, Linux Kernel, For Beginners, Learn Linux in easy steps, Fast! A Beginner's Guide Linux: Linux Guide for Beginners: Command Line, System and Operation (Linux Guide, Linux System, Beginners Operation Guide, Learn Linux Step-by-Step) Linux: Linux Mastery. The Ultimate Linux Operating System and Command Line Mastery (Operating System, Linux) Detection Estimation and Modulation Theory, Part I: Detection, Estimation, and Filtering Theory The Practice of Network Security Monitoring: Understanding Incident Detection and Response Host Response to Biomaterials: The Impact of Host Response on Biomaterial Selection Linux for Beginners: An Introduction to the Linux Operating System and Command Line Linux: The Ultimate Step by Step Guide to Quickly and Easily Learning Linux Linux Clustering: Building and Maintaining Linux Clusters Maximum Linux Security: A Hacker's Guide to Protecting Your Linux Server and Workstation The Linux Programming Interface: A Linux and UNIX System Programming Handbook Linux: Linux Bash Scripting - Learn Bash Scripting In 24 hours or less Ubuntu Linux: Your visual blueprint to using the Linux operating system SUSE Linux Enterprise Server Administration (Course 3112): CLA, LPIC - 1 & Linux+ Linux Apache Web Server Administration, Second Edition (Craig Hunt Linux Library) LINUX, UNIX, SAN, SYSTEM ADMINISTRATOR, LINUX SERVER ENGINEER, STORAGE ADMINISTRATOR LAST-MINUTE BOTTOM LINE JOB INTERVIEW PREPARATION QUESTIONS & ANSWERS Linux PCI Device Driver - A Template (Linux Driver Development) Linux Char Device Driver - A Template (Linux Driver Development) Data Matching: Concepts and Techniques for Record Linkage, Entity Resolution, and Duplicate Detection (Data-Centric Systems and Applications)