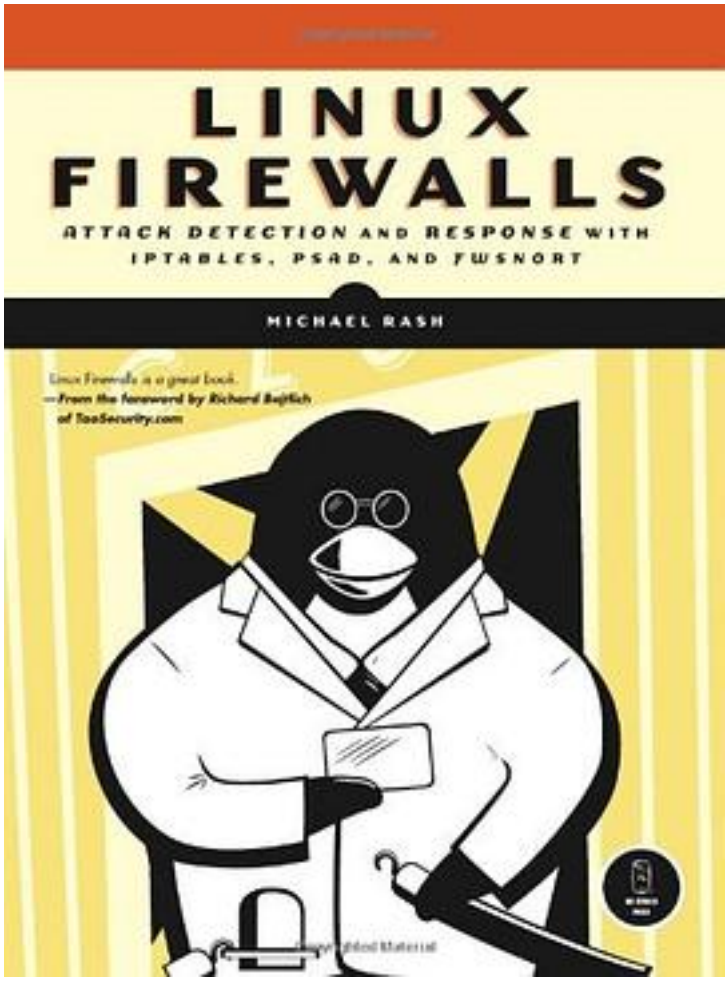
Linux Firewalls



Linux Firewalls_下载链接1_

著者:Michael Rash

出版者:No Starch Press

出版时间:2007.9

装帧:Paperback

isbn:9781593271411

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 fingerprinting iptables log analysis and policies Application layer attack detection with the iptables string match extension Building an iptables ruleset that emulates a Snort ruleset Port knocking vs. Single Packet Authorization (SPA) Tools for visualizing iptables logs Perl 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.

作者介绍:

Linux firewalls provide capabilities that rival commercial firewalls, and are built upon the powerful Netfilter infrastructure in the Linux kernel. Linux Firewalls: Attack Detection and Response explores using Netfilter as an intrusion detection system (IDS) by combining it with Snort rulesets and custom open source software created by the author. Providing concrete examples to illustrate concepts, the book discusses Linux firewall log analysis and policies, passive network authentication and authorization, exploit packet traces and Snort ruleset emulation, and more. Perl and C code snippets are included to help readers maximize the deployment of Linux firewalls as effective mechanisms for the detection and prevention of various network-based attacks.

目录: Introduction
Chapter 1: Care and Feeding of iptables
Chapter 2: Network Layer Attacks and Defense
Chapter 3: Transport Layer Attacks and Defense
Chapter 4: Application Layer Attacks and Defense
Chapter 5: Introducing psad: The Port Scan Attack Detector
Chapter 6: psad Operations: Detecting Suspicious Traffic
Chapter 7: Advanced psad Topics: From Signature Matching to OS Fingerprinting
Chapter 8: Active Response with psad
Chapter 9: Translating Snort Rules into iptables Rules
Chapter 10: Deploying Fwsnort
Chapter 11: Combining psad and Fwsnort
Chapter 12: Port-Knocking vs. Single Packet Authorization
Chapter 13: Introducing fwknop
Chapter 14: Visualizing iptables Logs
Appendix A: Attack Spoofing
Appendix B: A Complete fwsnort Script
・・・・・・(收起)

Linux Firewalls_下载链接1_

标签

linux

Firewalls

network

Linux

计算机

tangrui9105的计算机科学

第一梯队

外

评论

主要讲iptables，但是结合攻击的形式讲。以前和同事讨论过的一种攻击形式这里就讲到。

---
iptables的内容相对不多，主要还是副标题的内容。
大篇幅介绍了perl写的psad，fwsnort，fwknop，只能给个一般的评介。

Linux Firewalls_下载链接1_

书评

Linux Firewalls_下载链接1_