

Contents at a Glance

Contents ix

Preface xix

About the Author xxi

I: Packet Filtering and Basic Security Measures 1

- 1 Preliminary Concepts Underlying Packet-Filtering
Firewalls 3**
- 2 Packet-Filtering Concepts 25**
- 3 iptables: The Legacy Linux Firewall Administration
Program 51**
- 4 nftables: The Linux Firewall Administration
Program 83**
- 5 Building and Installing a Standalone Firewall 95**

II: Advanced Issues, Multiple Firewalls, and Perimeter Networks 143

- 6 Firewall Optimization 145**
- 7 Packet Forwarding 179**
- 8 NAT—Network Address Translation 197**
- 9 Debugging the Firewall Rules 211**
- 10 Virtual Private Networks 229**

III: Beyond iptables and nftables 235

- 11 Intrusion Detection and Response 237**
- 12 Intrusion Detection Tools 249**
- 13 Network Monitoring and Attack Detection 263**
- 14 Filesystem Integrity 295**

IV: Appendices 311**A Security Resources 313****B Firewall Examples and Support Scripts 315****C Glossary 351****D GNU Free Documentation License 363****Index 371**