Contents

Preface xix

About the Author xxii

I: Packet Filtering and Basic Security Measures 1

1 Preliminary Concepts Underlying Packet-Filtering Firewalls 3
   The OSI Networking Model 5
      Connectionless versus Connection-Oriented Protocols 7
      Next Steps 7
   The Internet Protocol 7
      IP Addressing and Subnetting 8
      IP Fragmentation 11
      Broadcasting and Multicasting 11
      ICMP 12
   Transport Mechanisms 14
      UDP 14
      TCP 14
   Don’t Forget Address Resolution Protocol 17
   Hostnames and IP Addresses 18
      IP Addresses and Ethernet Addresses 18
   Routing: Getting a Packet from Here to There 19
   Service Ports: The Door to the Programs on Your System 19
      A Typical TCP Connection: Visiting a Remote Website 20
   Summary 23

2 Packet-Filtering Concepts 25
   A Packet-Filtering Firewall 26
   Choosing a Default Packet-Filtering Policy 29
   Rejecting versus Denying a Packet 31
   Filtering Incoming Packets 31
      Remote Source Address Filtering 31
      Local Destination Address Filtering 34
Contents

Remote Source Port Filtering 35
Local Destination Port Filtering 35
Incoming TCP Connection State Filtering 35
Probes and Scans 36
Denial-of-Service Attacks 39
Source-Routed Packets 46
Filtering Outgoing Packets 46
Local Source Address Filtering 47
Remote Destination Address Filtering 47
Local Source Port Filtering 48
Remote Destination Port Filtering 48
Outgoing TCP Connection State Filtering 48
Private versus Public Network Services 49
Protecting Nonsecure Local Services 50
Selecting Services to Run 50
Summary 50

3 iptables: The Legacy Linux Firewall Administration Program 51
Differences between IPFW and Netfilter Firewall Mechanisms 51
IPFW Packet Traversal 52
Netfilter Packet Traversal 54
Basic iptables Syntax 54
iptables Features 55
NAT Table Features 58
mangle Table Features 60
iptables Syntax 61
filter Table Commands 62
filter Table Target Extensions 67
filter Table Match Extensions 68
nat Table Target Extensions 79
mangle Table Commands 81
Summary 82

4 nftables: The Linux Firewall Administration Program 83
Differences between iptables and nftables 83
Basic nftables Syntax 83
Enabling Common UDP Services 134

Accessing Your ISP’s DHCP Server
(UDP Ports 67, 68) 134

Accessing Remote Network Time Servers
(UDP Port 123) 136

Logging Dropped Incoming Packets 138

Logging Dropped Outgoing Packets 138

Installing the Firewall 139

Tips for Debugging the Firewall Script 139

Starting the Firewall on Boot with Red Hat
and SUSE 140

Starting the Firewall on Boot with Debian 141

Installing a Firewall with a Dynamic IP Address 141

Summary 141

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

6 Firewall Optimization 145

Rule Organization 145

Begin with Rules That Block Traffic on High
Ports 145

Use the State Module for ESTABLISHED
and RELATED Matches 146

Consider the Transport Protocol 146

Place Firewall Rules for Heavily Used Services
as Early as Possible 147

Use Traffic Flow to Determine Where to Place Rules
for Multiple Network Interfaces 147

User-Defined Chains 148

Optimized Examples 151

The Optimized iptables Script 151

Firewall Initialization 153

Installing the Chains 155

Building the User-Defined EXT-input
and EXT-output Chains 157

tcp-state-flags 165

connection-tracking 166

local-dhcp-client-query and
remote-dhcp-server-response 166
source-address-check 167
destination-address-check 168
Logging Dropped Packets with iptables 168
The Optimized nftables Script 170
Firewall Initialization 170
Building the Rules Files 172
Logging Dropped Packets with nftables 175
What Did Optimization Buy? 176
iptables Optimization 176
nftables Optimization 177
Summary 177

7 Packet Forwarding 179
The Limitations of a Standalone Firewall 179
Basic Gateway Firewall Setups 181
LAN Security Issues 182
Configuration Options for a Trusted Home LAN 183
   LAN Access to the Gateway Firewall 184
   LAN Access to Other LANs: Forwarding Local Traffic among Multiple LANs 186
Configuration Options for a Larger or Less Trusted LAN 188
   Dividing Address Space to Create Multiple Networks 188
   Selective Internal Access by Host, Address Range, or Port 190
Summary 195

8 NAT—Network Address Translation 197
The Conceptual Background of NAT 197
NAT Semantics with iptables and nftables 201
   Source NAT 203
   Destination NAT 205
Examples of SNAT and Private LANs 206
   Masquerading LAN Traffic to the Internet 206
   Applying Standard NAT to LAN Traffic to the Internet 208
Examples of DNAT, LANs, and Proxies 209
   Host Forwarding 209
Summary 210
9 Debugging the Firewall Rules 211
   General Firewall Development Tips 211
   Listing the Firewall Rules 213
      iptables Table Listing Example 213
      nftables Table Listing Example 216
   Interpreting the System Logs 217
      syslog Configuration 217
   Firewall Log Messages: What Do They Mean? 220
   Checking for Open Ports 223
      netstat -a [ -n -p -A inet ] 224
   Checking a Process Bound to a Particular Port with fuser 226
   Nmap 227
   Summary 227

10 Virtual Private Networks 229
   Overview of Virtual Private Networks 229
   VPN Protocols 229
      PPTP and L2TP 229
      IPsec 230
   Linux and VPN Products 232
      Openswan/Libreswan 233
      OpenVPN 233
   PPTP 233
   VPN and Firewalls 233
   Summary 234

III: Beyond iptables and nftables 235

11 Intrusion Detection and Response 237
   Detecting Intrusions 237
   Symptoms Suggesting That the System Might Be Compromised 238
      System Log Indications 239
      System Configuration Indications 239
      Filesystem Indications 240
      User Account Indications 240
      Security Audit Tool Indications 241
      System Performance Indications 241
What to Do If Your System Is Compromised 241
Incident Reporting 243
  Why Report an Incident? 243
  What Kinds of Incidents Might You Report? 244
  To Whom Do You Report an Incident? 246
  What Information Do You Supply? 246
Summary 247

12 Intrusion Detection Tools 249
  Intrusion Detection Toolkit: Network Tools 249
    Switches and Hubs and Why You Care 250
    ARPWatch 251
  Rootkit Checkers 251
    Running Chkrootkit 251
    What If Chkrootkit Says the Computer Is Infected? 253
    Limitations of Chkrootkit and Similar Tools 253
    Using Chkrootkit Securely 254
    When Should Chkrootkit Be Run? 255
  Filesystem Integrity 255
  Log Monitoring 256
    Swatch 256
  How to Not Become Compromised 257
    Secure Often 257
    Update Often 258
    Test Often 259
Summary 261

13 Network Monitoring and Attack Detection 263
  Listening to the Ether 263
    Three Valuable Tools 264
  TCPDump: A Simple Overview 265
    Obtaining and Installing TCPDump 266
    TCPDump Options 267
    TCPDump Expressions 269
    Beyond the Basics with TCPDump 272
Contents

Using TCPDump to Capture Specific Protocols 272
Using TCPDump in the Real World 272
Attacks through the Eyes of TCPDump 280
Recording Traffic with TCPDump 284
Automated Intrusion Monitoring with Snort 286
Obtaining and Installing Snort 287
Configuring Snort 288
Testing Snort 289
Receiving Alerts 290
Final Thoughts on Snort 291
Monitoring with ARPWatch 291
Summary 293

14 Filesystem Integrity 295
Filesystem Integrity Defined 295
Practical Filesystem Integrity 295
Installing AIDE 296
Configuring AIDE 297
Creating an AIDE Configuration File 297
A Sample AIDE Configuration File 299
Initializing the AIDE Database 300
Scheduling AIDE to Run Automatically 301
Monitoring AIDE for Bad Things 301
Cleaning Up the AIDE Database 302
Changing the Output of the AIDE Report 303
Obtaining More Verbose Output 305
Defining Macros in AIDE 306
The Types of AIDE Checks 307
Summary 310

IV: Appendices 311

A Security Resources 313
Security Information Sources 313
Reference Papers and FAQs 314

B Firewall Examples and Support Scripts 315
iptables Firewall for a Standalone System from Chapter 5 315