

Table of Contents

About the Authorxiii

About the Technical Reviewerxv

Acknowledgmentsxvii

Introductionxix

Part I: System Programming 1

Chapter 1: System Calls3

 Source Code..... 3

 What Is a System Call? 4

 C System Call5

 sys/unix Package 8

 System Call in Go..... 10

 Summary..... 14

Chapter 2: System Calls Using Go.....15

 Source Code..... 15

 Syscall Package 16

 syscall Application..... 16

 Checking Disk Space 18

 Webserver with syscall..... 20

ELF Package.....22

 High-Level ELF Format23

 Dump Example24

/sys Filesystem28

 Reading AppArmor.....29

Summary.....31

Chapter 3: Accessing proc File System33

Source Code.....33

Peeking Inside procfs.....34

Reading Memory Information38

 Peeking Network Information.....41

Using the procfs Library.....44

 Code Sample44

 Inside the procfs Library.....46

Summary.....48

Part II: Containers.....49

Chapter 4: Simple Containers.....51

Linux Namespace.....51

cgroups55

rootfs.....58

Gontainer Project63

Summary.....70

Chapter 5: Containers with Networking71

Source Code.....71

 Network Namespace72

 Setting Up with the ip Tool.....74

 Containers with Networks79

Summary88

Chapter 6: Docker Security.....89

Source Code.....89

seccomp Profiles89

 libseccomp91

 Docker seccomp.....95

Docker Proxy.....98

Container Attack Surface105

Summary.....106

Part III: Application Security109

Chapter 7: Gosec and AST111

Source Code.....111

Abstract Syntax Tree111

 Modules115

 Sample Code116

gosec122

 Inside gosec123

 Rules.....128

Summary.....130

Chapter 8: Scorecard.....131

Source Code..... 131

What Is Scorecard?..... 131

 Setting Up Scorecard..... 133

 Running Scorecard..... 137

 High-Level Flow..... 139

GitHub..... 145

 GitHub API..... 145

 GitHub Explorer..... 156

Summary..... 159

Part IV: Networking161

Chapter 9: Simple Networking.....163

Source Code..... 163

TCP Networking..... 163

 TCP Client..... 164

 TCP Server..... 166

UDP Networking..... 168

 UDP Client..... 169

 UDP Server..... 172

 Concurrent Servers..... 174

Load Testing..... 175

Summary..... 179

Chapter 10: System Networking.....181

Source Code..... 181

Ping Utility..... 181

 Code Walkthrough..... 182

DNS Server..... 188

 Running a DNS Server..... 188

 DNS Forwarder..... 189

 Pack and Unpack..... 193

Summary..... 196

Chapter 11: Google gopacket.....199

Source Code..... 199

gopacket..... 200

 Layer..... 200

 Packet..... 204

Using gopacket..... 205

 pcap..... 205

 Networking Sniffer..... 206

 Capturing With BPF..... 217

Summary..... 222

Chapter 12: Epoll Library.....223

Source Code..... 224

Understanding epoll..... 224

epoll in Golang..... 226

 Epoll Registration..... 227

 Epoll Wait..... 229

Epoll Library..... 232

Summary..... 235

Part V: Securing Linux239

Chapter 13: Vulnerability Scanner239

Source Code 239

Vulnerability Scanners 240

Using Vuls..... 241

 Checking Out the Code 241

 Running Scan 243

Learning From Vuls 248

 Port Scan 248

 Exec 255

 SQLite 257

Summary..... 263

Chapter 14: CrowdSec265

Source Code 265

CrowdSec Project..... 266

 Using CrowdSec 266

 crowdsec.db 270

Learning From CrowdSec..... 273

 System Signal Handling..... 274

 Handling Service Dependencies..... 280

 GeolP Database 285

Summary..... 290

Part VI: Terminal User Interface.....293

Chapter 15: ANSI and UI293

Source Code..... 293

ANSI Escape Code..... 294

ANSI-Based UI..... 296

 Color Table 296

 Styling Text 299

Open Source Library 300

 Gookit 300

 Spinner 303

Summary..... 306

Chapter 16: TUI Framework.....307

 uiprogress 307

 Code Flow 309

 Updating Progress 310

Bubbletea..... 313

 Init..... 315

 Update 318

 View..... 319

Summary..... 321

Part VII: Linux System325

Chapter 17: systemd.....325

Source Code..... 325

 systemd 325

 systemctl 329

 Hello Server systemd..... 332

TABLE OF CONTENTS

go-systemd Library	334
Summary	345
Chapter 18: cadvisor	347
Source Code.....	347
Running cAdvisor	347
Web User Interface.....	352
Architecture	355
Initialization.....	357
Manager	361
Monitoring Filesystem.....	368
Information from /sys and /proc	371
Client Library.....	375
Summary.....	375
Index.....	377