The Foundations of Website Architecture series

- Understand networks, Web servers, and clients
- Secure your site for e-commerce
- Work toward your Webmaster Certification

ADMINISTRATING

Web Servers, Security, & Maintenance

Interactive Workbook

Suranaree University of Technology
31051000656344

ERIC LARSON · BRIAN STEPHENS

CONTENTS

From the Editor xiii

Executive Foreword xv

Introduction xvii

About the Authors xxiii

PART I WEB SERVER ADMINISTRATION

CHAPTER 1 What Is a Web Server? 1

Lab 1.1 Client/Server Basics 2
- 1.1.1 Understand Client/Server Concepts 4
- 1.1.2 Describe Basic Functionality of Web Servers and Browsers 5

Lab 1.2 Electronic Publishing 10
- 1.2.1 Understand the Basics of Creating Hypertext Documents 13
- 1.2.2 Understand the Difference Between ASCII and Binary Files 14
- 1.2.3 Give Examples of MIME Types 14

Lab 1.3 HTTP Overview 19
- 1.3.1 Identify the Parts of an HTTP Transaction 25
- 1.3.2 Identify HTTP Request Methods 25
- 1.3.3 Identify HTTP Headers and Server Responses 25

Lab 1.4 Other Web-Related Servers 29
- 1.4.1 Understand the Functionality of Proxy Servers 34
- 1.4.2 Identify Other Services that May Run Alongside an HTTP Server 34

Test Your Thinking 37

CHAPTER 2 Planning Your Server 39

Lab 2.1 Hosting Your Site 40
2.1.1 Determine How to Host Your Site 46
Lab 2.2 Hosting Your Own Server 49
2.2.1 Understand What Is Required to Put a Server on the Internet 54
Lab 2.3 UNIX vs. NT 57
2.3.1 Understand the Major Differences Between Windows NT and UNIX 62
2.3.2 Determine Which Operating System Best Fits Your Needs 62
Lab 2.4 Sizing Your Server 65
2.4:1 Determine Size and Bandwidth Requirements for Your Server 68
2.4.2 Understand How to Spot and Resolve Performance Problems 68
Lab 2.5 Domain Names 72
2.5.1 Register a Domain 75
Test Your Thinking 78

CHAPTER 3 Users and Documents 81

Lab 3.1 Server Users and Directories 82
3.1.1 Enable Users to Publish Documents on a Server 85
3.1.2 Understand How URLs Are Mapped to Files 86
Lab 3.2 Server Administrators 88
3.2.1 Understand the Roles and Responsibilities of a System Administrator 92
Lab 3.3 Document Hierarchy 94
3.3.1 Understand How Documents Are Linked and Organized in the File System 97
3.3.2 Understand How the Web Server Locates a Requested Document 98
Lab 3.4 Directory Indexing 100
3.4.1 Understand Directory Indexes 102
Lab 3.5 File and Directory Names 106
3.5.1 Choose Appropriate Names for Files and Directories 108

Lab 3.6 Transferring Files 111
3.6.1 Understand How Files Are Transferred to a Web Server 115
3.6.2 Understand FrontPage Extensions 116
Test Your Thinking 120

CHAPTER 4 Server Configuration 121

Lab 4.1 Choosing Web Server Software 122
4.1.1 Understand What Options Are Available for Server Software 132
4.1.2 Install a Web Server on Your Computer 133
Lab 4.2 Customizing Your Web Server 137
4.2.1 Understand Typical Server Configuration Options 140
Lab 4.3 Controlling Access 144
4.3.1 Set Proper Permissions on Files and Directories 146
4.3.2 Limit Access on Your Server to Specific Users and Hosts 146
Lab 4.4 Secure Sockets Layer Configuration 150
4.4.1 Understand How the Secure Sockets Layer Is Used 153
Lab 4.5 Virtual Hosts 155
4.5.1 Understand the Basics of Virtual Hosting 156
4.5.2 Understand How to Configure Virtual Hosts On Your Server 156
Test Your Thinking 160

CHAPTER 5 Server-Side Programming 161

Lab 5.1 Dynamic Documents 162
5.1.1 Understand Why Programs Are Used to Generate Documents 163
Lab 5.2 CGI and Forms 166
5.2.1 Understand What CGI Is and How CGI Programs Work 169
5.2.2 Understand How HTML Forms Are Used 170
Lab 5.3 Server-Side Includes 175
5.3.1 Understand Parsed HTML 177

Lab 5.4 Active Server Pages 181
5.4.1 Understand How Active Server Pages Work 182
Lab 5.5 Servlets and Java Server Pages 185
5.5.1 Understand the Benefits of Servlets and JSP 187
Test Your Thinking 192

CHAPTER 6 Log Files 193

Lab 6.1 Log File Formats 194
6.1.1 Understand How to Configure Logging 197
6.1.2 Understand How to Read Different Server Log Files 197
Lab 6.2 Referrers 202
6.2.1 Understanding How People Are Getting to Your Site 203
Lab 6.3 Being Proactive 207
6.3.1 Use Log File to Help Find Dead Links 209
6.3.2 Understand How to Spot Suspicious Activity 210
Lab 6.4 Statistics 213
6.4.1 Determine How Many People Have Been Visiting Your Site 216
Test Your Thinking 220

CHAPTER 7 Search Engines, Robots, and Automation 221

Lab 7.1 Search Engines 222
7.1.1 Understand How to Create a Searchable Site 225
Lab 7.2 Publicizing Your Site 228
7.2.1 Publicize Your Site Effectively 230
Lab 7.3 Robots and Spiders 235
7.3.1 Control How Search Engines Access Your Site 237
Lab 7.4 Automation 241
7.4.1 Determine How to Automate Administrative Tasks 243
Test Your Thinking 246

PART II WEB SECURITY

CHAPTER 8 Introduction to Security 247

Lab 8.1 Why We Need Security 248
8.1.1 Understand the Need for Security 250
Lab 8.2 Types of Attacks and Vulnerabilities 255
8.2.1 Identify Various Types of Attacks 258
8.2.2 Understand Various Types of Attacks 259
Lab 8.3 Security Resources 266
8.3.1 Find the Security Risks that Pertain to Your Site 270
8.3.2 Explore the CERT Coordination Center Advisories 271
8.3.3 Find Other Security Resources 272
Lab 8.4 Security Basics 280
8.4.1 Understand the Basic Rules of Security 282
Test Your Thinking 286

CHAPTER 9 Network Security 287

Lab 9.1 Networking Basics 288
9.1.1 Understand IP Addresses and Netmasks 295
9.1.2 Identify IP Addresses on the Same Subnet 296
9.1.3 Dissect an IP Packet 296
Lab 9.2 Packet Sniffing 302
9.2.1 Use a Packet Sniffer 304
9.2.2 Understand the Risks of Packet Sniffing 305
9.2.3 Determine What Data is Sent in an HTTP Packet 306
Lab 9.3 Other Network Vulnerabilities 313
9.3.1 Understand IP Spoofing 317
9.3.2 Understand Network Denial of Service Attacks 317
9.3.3 Understand Other Network Attacks 318
Lab 9.4 Firewalls and Proxies 324
9.4.1 Understand the Benefit of Filtering by IP and Port 327
9.4.2 Understand the Limitations of Firewalls 329
9.4.3 Understand Other Benefits Firewalls Provide 329
Test Your Thinking 334

CHAPTER 10 Web Server Security 335

Lab 10.1 Host/OS Hardening 336
- 10.1.1 Determine What Is Running on Your Machine 343
- 10.1.2 Determine Which Ports Accept Connections 343

Lab 10.2 Who to Run a Web Server As 347
- 10.2.1 Set up a Safe User to Run the Web Server As 349
- 10.2.2 Modify the User the Web Server Runs As 350

Lab 10.3 File Permissions and Ownership 356
- 10.3.1 Understand File Permissions and Ownership 358
- 10.3.2 Understand Risks of Web Server File Ownership 360
- 10.3.3 Protect Against the Risks of Directory Browsing 360

Lab 10.4 Other Configuration Concerns 369
- 10.4.1 Understand the Risks Symbolic Links Present 373
- 10.4.2 Understand the Risks with Server Side Includes 374

Test Your Thinking 378

CHAPTER 11 CGI Security 379

Lab 11.1 Who to Run CGI As 380
- 11.1.1 Determine a Safe User to Run CGI As 382

Lab 11.2 Poor CGI Programming 389
- 11.2.1 Identify Risks from Poor Programming 390

Lab 11.3 Tainted CGI Variables 396
- 11.3.1 Check for Unsafe Characters in CGI Input 398
- 11.3.2 Check for Safe Characters in CGI Input 399
- 11.3.3 Work Around Unsafe Characters in CGI Input 400

Lab 11.4 Buffer Overflows 405
- 11.4.1 Understand What Happens with a Buffer Overflow 408

Lab 11.5 Other CGI Risks 413
- 11.5.1 Use Referrers for Added CGI Protection 416
- 11.5.2 Understand the Risks of .cgi File Extensions 417

Test Your Thinking 422

CHAPTER 12 Web Client Security 423

Lab 12.1 Java Applets 424
- 12.1.1 Understand What Applets Can and Can't Do 426

CHAPTER 10 Web Server Security 335

Lab 10.1 Host/OS Hardening 336
10.1.1 Determine What Is Running on Your Machine 343
10.1.2 Determine Which Ports Accept Connections 343

Lab 10.2 Who to Run a Web Server As 347
10.2.1 Set up a Safe User to Run the Web Server As 349
10.2.2 Modify the User the Web Server Runs As 350

Lab 10.3 File Permissions and Ownership 356
10.3.1 Understand File Permissions and Ownership 358
10.3.2 Understand Risks of Web Server File Ownership 360
10.3.3 Protect Against the Risks of Directory Browsing 360

Lab 10.4 Other Configuration Concerns 369
10.4.1 Understand the Risks Symbolic Links Present 373
10.4.2 Understand the Risks with Server Side Includes 374
Test Your Thinking 378

CHAPTER 11 CGI Security 379

Lab 11.1 Who to Run CGI As 380
11.1.1 Determine a Safe User to Run CGI As 382

Lab 11.2 Poor CGI Programming 389
11.2.1 Identify Risks from Poor Programming 390

Lab 11.3 Tainted CGI Variables 396
11.3.1 Check for Unsafe Characters in CGI Input 398
11.3.2 Check for Safe Characters in CGI Input 399
11.3.3 Work Around Unsafe Characters in CGI Input 400

Lab 11.4 Buffer Overflows 405
11.4.1 Understand What Happens with a Buffer Overflow 408

Lab 11.5 Other CGI Risks 413
11.5.1 Use Referrers for Added CGI Protection 416
11.5.2 Understand the Risks of .cgi File Extensions 417
Test Your Thinking 422

CHAPTER 12 Web Client Security 423

Lab 12.1 Java Applets 424
12.1.1 Understand What Applets Can and Can't Do 426

12.1.2 Understand What a Hostile Java Applet Is 427
12.1.3 Protect Yourself from Java Applets 428

Lab 12.2 ActiveX 437
12.2.1 Understand the Risks ActiveX Poses 440
12.2.2 Protect Yourself from ActiveX 441

Lab 12.3 JavaScript 447
12.3.1 Understand the Risks JavaScript Poses 449
12.3.2 Protect Yourself from JavaScript 450

Lab 12.4 Cookies 454
12.4.1 Understand the Risk That Cookies Pose 456
12.4.2 Protect Yourself from Cookies 457
Test Your Thinking 464

CHAPER 13 Secure Online Transactions 465

Lab 13.1 Encryption 466
13.1.1 Understand Weaknesses in Cryptography 472

Lab 13.2 Secure Socket Layer 477
13.2.1 Understand the Advantage of SSL 479
13.2.2 Identify Careless Use of SSL 480

Lab 13.3 Certificate Authorities 483
13.3.1 Understand What a Certificate Is 485
13.3.2 Obtain Your Own Certificate 486

Lab 13.4 Access Control Lists 490
13.4.1 Understand How ACLs Work 492
13.4.2 Understand the Benefits ACLs Provide 493
Test Your Thinking 499

CHAPTER 14 Intrusion Detection and Recovery 501

Lab 14.1 Detecting an Attack 502
14.1.1 Monitor Logs for Strange Behavior 504
14.1.2 Determine if the System is Acting Abnormally 505
14.1.3 Detect a Change in the System Configuration 506

Lab 14.2 Recovering from an Attack 515
14.2.1 Collect Evidence for Prosecution 517

14.2.2 Report an Attack 517
14.2.3 Properly Restore to a Safe Configuration 518
Test Your Thinking 525

Appendix A Answers to Self-Review Questions 527

Appendix B ASCII Values 549

Appendix C Well-Known Port Numbers 551

Appendix D Base Conversion 552

Appendix E Packet Formats 557

Index 559