

CONTENTS

Introduction *xix*

PART I **SECURING THE INFRASTRUCTURE** **1**

CHAPTER 1 **Infrastructure Security in the Real World** **3**

Security Challenges	3
Infrastructure Security Scenario 1.....	4
Infrastructure Security Scenario 2.....	6
Summary.....	8

CHAPTER 2 **Understanding Access-Control and Monitoring Systems** **9**

A Quick Primer on Infrastructure Security.....	9
Access Control.....	12
Security Policies	14
Physical Security Controls.....	15
Locks and Keys.....	16
Standard Key-Locking Deadbolts	17
Solenoid-Operated Deadbolt Locks.....	18
Cipher Locks.....	19
Access-Control Gates	20
Sliding Gates	20
Swinging Gates	21
Control Relays	21
Authentication Systems	23
Magnetic Stripe Readers	24
Smart Cards	25
RFID Badges.....	26
Biometric Scanners	27
Remote-Access Monitoring.....	29
Opened- and Closed-Condition Monitoring	30
Automated Access-Control Systems	32

Hands-On Exercises	33
Discussion	34
Procedure	35
Review Questions	43

CHAPTER 3 Understanding Video Surveillance Systems 45

Video Surveillance Systems	45
Cameras	46
Hands-On Exercises	60
Discussion	61
Procedure	61
Review Questions	69

CHAPTER 4 Understanding Intrusion-Detection and Reporting Systems 71

Intrusion-Detection and Reporting Systems	71
Security Controllers	74
Sensors	77
Vehicle-Detection Sensors	82
Fire-Detection Sensors	85
Output Devices	87
Hands-On Exercises	90
Discussion	90
Procedure	92
Review Questions	94

CHAPTER 5 Infrastructure Security: Review Questions and Hands-On Exercises 97

Summary Points	97
Security Challenge Scenarios	101
Infrastructure Security Scenario 1	101
Infrastructure Security Scenario 2	102
Professional Feedback	102
Review Questions	107
Exam Questions	109

PART II	SECURING LOCAL HOSTS	113
CHAPTER 6	Local Host Security in the Real World	115
	Security Challenges	115
	Computing Device Security Scenario 1	116
	Computing Device Security Scenario 2	117
	Summary.....	120
CHAPTER 7	Securing Devices	121
	The Three Layers of Security	121
	Securing Host Devices	123
	Securing Outer-Perimeter Portals	124
	Additional Inner-Perimeter Access Options	127
	Hands-On Exercises	137
	Objectives	137
	Procedure	137
	Review Questions.....	148
CHAPTER 8	Protecting the Inner Perimeter	149
	The Inner Perimeter	149
	Operating Systems	151
	Operating System Security Choices	168
	Common Operating System Security Tools	169
	Using Local Administrative Tools	177
	Implementing Data Encryption.....	182
	Hands-On Exercises	188
	Objectives	188
	Resources	188
	Discussion	189
	Procedures	190
	Tables	200
	Lab Questions.....	201
CHAPTER 9	Protecting Remote Access	203
	Protecting Local Computing Devices	203
	Using a Secure Connection	204

Establishing and Using a Firewall	204
Installing and Using Anti-Malware Software	205
Removing Unnecessary Software	205
Disabling Nonessential Services	205
Disabling Unnecessary OS Default Features	205
Securing the Web Browser	205
Applying Updates and Patches	206
Requiring Strong Passwords	206
Implementing Local Protection Tools	206
Software-Based Local Firewalls	207
Using Local Intrusion-Detection Tools	209
Profile-Based Anomaly-Detection Systems	210
Threshold-Based Anomaly-Detection Systems	211
Configuring Browser Security Options	211
Configuring Security Levels	213
Configuring Script Support	214
Defending Against Malicious Software	218
Using Antivirus Programs	220
Using Antispyware	221
Hardening Operating Systems	222
Service Packs	222
Patches	222
Updates	223
Overseeing Application Software Security	223
Software Exploitation	223
Applying Software Updates and Patches	224
Hands-On Exercises	225
Objectives	225
Resources	225
Discussion	225
Procedures	226
Tables	241
Lab Questions	242

CHAPTER 10**Local Host Security: Review Questions and Hands-On Exercises****243**

Summary Points	243
Security Challenge Scenarios	248

Computing Device Security Scenario 1	248
Computing Device Security Scenario 2	248
Professional Feedback	248
Review Questions	257
Exam Questions	259

PART III SECURING LOCAL NETWORKS 263

CHAPTER 11 Local Network Security in the Real World 265

Security Challenges	266
Local Network Security Scenario 1.....	266
Local Network Security Scenario 2.....	270
Summary.....	272

CHAPTER 12 Networking Basics 273

Understanding the Basics of Networking	273
Campus Area Networks or Corporate Area Networks (CANs)	274
Metropolitan Area Networks (MANs)	274
Wireless Local Area Networks (WLANs)	274
Storage Area Networks (SANs)	274
The OSI Networking Model	275
Layer 1: Physical	276
Layer 2: Data Link	276
Layer 3: Network	276
Layer 4: Transport	276
Layer 5: Session	276
Layer 6: Presentation	277
Layer 7: Application	277
Data Transmission Packets.....	277
OSI Layer Security	278
Network Topologies.....	280
Bus Topology	280
Ring Topology.....	280
Star Topology	281
Mesh Topology	282
Logical Topologies	282
Hands-On Exercises	283

	Objectives	283
	Resources	283
	Discussion	283
	Procedure	284
	Lab Questions.....	295
	Lab Answers	295
CHAPTER 13	Understanding Networking Protocols	297
	The Basics of Networking Protocols	297
	MAC Addresses	298
	TCP/IP.....	299
	Ethernet	309
	Network Control Strategies	311
	Hands-On Exercises	313
	Objectives	313
	Discussion	313
	Procedures	314
	Lab Questions.....	325
	Lab Answers	326
CHAPTER 14	Understanding Network Servers	327
	The Basics of Network Servers.....	327
	Server Security.....	330
	Network Administrators	331
	Server Software Security.....	335
	User Accounts.....	341
	Network Authentication Options	347
	Establishing Resource Controls	348
	Maintaining Server Security.....	352
	Vulnerability Scanning	358
	Hands-On Exercises	361
	Objectives	361
	Resources	361
	Discussion	362
	Procedures	362
	Lab Questions.....	382
	Lab Answers	382

CHAPTER 15	Understanding Network Connectivity Devices	385
	Network Switches	386
	Routers	388
	Gateways	390
	Network Bridges	391
	Wireless Network Connectivity	392
	Network Connectivity Device Vulnerabilities	392
	Network Connectivity Device Attacks	393
	Network Connectivity Defense	397
	Network Hardening	398
	Hands-On Exercises	399
	Objectives	399
	Resources	399
	Procedures	399
	Lab Questions	404
	Lab Answers	404
CHAPTER 16	Understanding Network Transmission Media Security	407
	The Basics of Network Transmission Media	407
	Copper Wire	408
	Light Waves	410
	Wireless Signals	412
	Transmission Media Vulnerabilities	415
	Securing Wireless Networks	415
	Hands-On Exercises	417
	Objectives	417
	Resources	417
	Procedure	417
	Lab Questions	421
	Lab Answers	421
CHAPTER 17	Local Network Security: Review Questions	423
	Summary Points	423
	Security Challenge Scenarios	432
	Local Network Security Scenario 1	432
	Local Network Security Scenario 2	432
	Professional Feedback	432
	Review Questions	443

PART IV	SECURING THE PERIMETER	449
<hr/>		
CHAPTER 18	Perimeter Security in the Real World	451
<hr/>		
	Security Challenges	451
	Internet Security Scenario 1	451
	Internet Security Scenario 2	454
	Summary	455
CHAPTER 19	Understanding the Environment	457
<hr/>		
	The Basics of Internet Security	457
	Understanding the Environment	460
	Basic Internet Concepts	461
	Internet Services	468
	Standards and RFCs	470
	Hands-On Exercises	471
	Objectives	471
	Resources	472
	Discussion	472
	Procedures	472
	Lab Questions	486
	Lab Answers	486
CHAPTER 20	Hiding the Private Network	487
<hr/>		
	Understanding Private Networks	487
	Network Address Translation	488
	Port Address Translation	489
	Port Forwarding or Mapping	490
	Network Segmentation	492
	Software-Defined Networking	494
	Hands-On Exercises	496
	Objectives	496
	Resources	496
	Discussion	496
	Procedure	497
	Lab Questions	508
	Lab Answers	509

CHAPTER 21	Protecting the Perimeter	511
	Understanding the Perimeter	511
	Firewalls	515
	Firewall Considerations	517
	Network Appliances	519
	Proxy Servers	520
	Demilitarized Zones (DMZs)	522
	Single-Firewall DMZs	523
	Dual-Firewall DMZs	524
	Honeypots	525
	Extranets	526
	Hands-On Exercises	528
	Objectives	528
	Resources	528
	Procedures	528
	Lab Questions	534
	Lab Answers	534
CHAPTER 22	Protecting Data Moving Through the Internet	535
	Securing Data in Motion	535
	Authentication	536
	Encryption	542
	Cryptography	543
	Digital Certificates	545
	Hash Tables	548
	Cookies	548
	CAPTCHAs	549
	Virtual Private Networks	550
	Hands-On Exercises	552
	Objectives	552
	Resources	552
	Discussion	552
	Procedures	552
	Lab Questions	563
	Lab Answers	563

CHAPTER 23	Tools and Utilities	565
	Using Basic Tools	565
	IFconfig/IPconfig	565
	Whois	566
	Nslookup	567
	PING	567
	Traceroute	568
	Telnet	569
	Secure Shell	570
	Monitoring Tools and Software	570
	Nagios	572
	SolarWinds	572
	Microsoft Network Monitor	572
	Wireshark	572
	Snort	573
	Nmap	575
	Nikto	575
	OpenVAS	575
	Metasploit	575
	The Browser Exploitation Framework (BeEF)	576
	Other Products	576
	Hands-On Exercises	578
	Objectives	578
	Resources	578
	Discussion	578
	Procedures	579
	Capturing a PING	583
	Lab Questions	589
	Lab Answers	589
CHAPTER 24	Identifying and Defending Against Vulnerabilities	591
	Zero Day Vulnerabilities	591
	Software Exploits	592
	SQL Injection	594
	Java	597
	Other Software Exploits	599
	Social Engineering Exploits	600

Phishing Attacks	600
Network Threats and Attacks	603
Broadcast Storms	603
Session-Hijacking Attacks	604
Dictionary Attacks	606
Denial of Service (DoS) Attacks	606
Tarpitting	611
Spam	612
Protecting Against Spam Exploits	613
Other Exploits	614
Transport Layer Security (TLS) Exploits	614
FREAK Exploits	615
Logjam Exploits	615
Hands-On Exercises	616
Objectives	616
Resources	616
Discussion	616
Procedures	616

CHAPTER 25**Perimeter Security: Review Questions
and Hands-On Exercises****627**

Summary Points	627
Security Scenario Review	637
Network Security Scenario 1	637
Network Security Scenario 2	637
Professional Feedback	637
Review Questions	644
Exam Questions	647
<i>Appendix A</i>	<i>651</i>
<i>Appendix B</i>	<i>703</i>
<i>Appendix C</i>	<i>715</i>
<i>Index</i>	<i>727</i>