

Contents

<i>Introduction</i>		<i>xxiii</i>
<i>Assessment Test</i>		<i>xxxix</i>
Chapter 1	General Security Concepts	1
	Understanding Information Security	3
	Securing the Physical Environment	4
	Examining Operational Security	5
	Working with Management and Policies	7
	Understanding the Goals of Information Security	12
	Comprehending the Security Process	13
	Appreciating Antivirus Software	13
	Implementing Access Control	14
	Understanding Authentication	15
	Authentication Issues to Consider	21
	Distinguishing between Security Topologies	22
	Setting Design Goals	23
	Creating Security Zones	26
	Working with Newer Technologies	29
	Addressing Business Concerns	33
	Dealing with Telephony Issues	38
	Summary	39
	Exam Essentials	40
	Hands-On Labs	43
	Lab 1.1: Update a Linux System	43
	Lab 1.2: Update a Windows-Based System	43
	Review Questions	44
	Answers to Review Questions	48
Chapter 2	Identifying Potential Risks	51
	Calculating Attack Strategies	53
	Understanding Access Attack Types	54
	Recognizing Modification and Repudiation Attacks	55
	Identifying Denial-of-Service and Distributed Denial-of-Service Attacks	56
	Recognizing Common Attacks	58
	Back Door Attacks	59
	Spoofing Attacks	60
	Man-in-the-Middle Attacks	60
	Replay Attacks	62
	Password-Guessing Attacks	62
	Privilege Escalation	63

Identifying TCP/IP Security Concerns	64
Working with the TCP/IP Suite	65
Understanding Encapsulation	68
Working with Protocols and Services	69
Recognizing TCP/IP Attacks	72
Understanding Software Exploitation	78
Understanding OVAL	81
Surviving Malicious Code	81
Viruses	81
Trojan Horses	88
Logic Bombs	88
Worms	89
Antivirus Software	89
Understanding Social Engineering	91
Introducing Auditing Processes and Files	93
Summary	94
Exam Essentials	95
Hands-On Labs	98
Lab 2.1: Identify Running Processes on a Windows-Based Machine	98
Lab 2.2: Identify Running Processes on a Linux-Based Machine	98
Review Questions	100
Answers to Review Questions	104
Chapter 3 Infrastructure and Connectivity	107
Understanding Infrastructure Security	109
Working with Hardware Components	110
Working with Software Components	112
Understanding the Different Network Infrastructure Devices	113
Firewalls	113
Hubs	118
Modems	118
Remote Access Services	119
Routers	120
Switches	122
Telecom/PBX Systems	122
Virtual Private Networks	124
Wireless Access Points	125
Monitoring and Diagnosing Networks	127
Network Monitors	127
Intrusion Detection Systems	128
Securing Workstations and Servers	129
Understanding Mobile Devices	130

Understanding Remote Access	132
Using Point-to-Point Protocol	132
Working with Tunneling Protocols	133
Using 802.1x Wireless Protocols	135
Working with RADIUS	135
TACACS/+	136
Securing Internet Connections	136
Working with Ports and Sockets	136
Working with E-Mail	137
Working with the Web	139
Working with File Transfer Protocol	144
Understanding Network Protocols	146
The Basics of Cabling, Wires, and Communications	147
Coax	148
Unshielded Twisted Pair and Shielded Twisted Pair	150
Fiber Optic	152
Infrared	154
Radio Frequencies	154
Microwave Systems	154
Employing Removable Storage	156
CD-R/DVD-R	157
Diskettes	157
Flash Cards	158
Hard Drives	158
Network Attached Storage	158
Smart Cards	159
Tape	159
Thumb Drives	161
Summary	161
Exam Essentials	162
Hands-On Labs	164
Lab 3.1: Examine the Windows Routing Table	164
Lab 3.2: Examine the Linux Routing Table	164
Review Questions	165
Answers to Review Questions	169
Chapter 4	Monitoring Activity and Intrusion Detection
	171
Monitoring the Network	173
Recognizing the Different Types of Network Traffic	174
Monitoring Network Systems	178
Understanding Intrusion Detection Systems	179
Working with a Network-Based IDS	184
Working with a Host-Based IDS	189
Working with NIPS	190
Utilizing Honeypots	191
Understanding Incident Response	192

Working with Wireless Systems	198
Wireless Transport Layer Security	198
IEEE 802.11x Wireless Protocols	199
WEP/WAP	200
Wireless Vulnerabilities to Know	201
Understanding Instant Messaging's Features	202
Understanding IM Vulnerabilities	203
Controlling Privacy	204
Working with 8.3 File Naming	204
Understanding Protocol Analyzers	205
Understanding Signal Analysis and Intelligence	205
Footprinting	206
Scanning	206
Summary	207
Exam Essentials	208
Hands-On Labs	210
Lab 4.1: View the Active TCP and UDP Ports	210
Lab 4.2: Run Windows Network Monitor	210
Lab 4.3: Install snort in Linux	211
Lab 4.4: Make File Extensions Visible in Windows XP	211
Lab 4.5: Monitor Network Traffic in Linux	211
Review Questions	213
Answers to Review Questions	217
Chapter 5	Implementing and Maintaining a Secure Network 219
Overview of Network Security Threats	221
Defining Security Baselines	222
Hardening the OS and NOS	224
Configuring Network Protocols	225
Hardening Microsoft Windows Vista	227
Hardening Microsoft Windows XP	228
Hardening Windows Server 2003	229
Hardening Microsoft Windows 2000	230
Hardening Unix/Linux	231
Hardening Novell NetWare	232
Hardening Apple Macintosh	233
Hardening Filesystems	234
Updating Your Operating System	237
Hardening Network Devices	238
Updating Network Devices	238
Configuring Routers and Firewalls	239
Hardening Applications	240
Hardening Web Servers	240
Hardening E-Mail Servers	241
Hardening FTP Servers	242
Hardening DNS Servers	243

	Hardening NNTP Servers	244
	Hardening File and Print Servers and Services	245
	Hardening DHCP Services	246
	Working with Data Repositories	246
	Summary	251
	Exam Essentials	252
	Hands-On Labs	254
	Lab 5.1: Install OpenLDAP on a SuSE Server	254
	Lab 5.2: Work with Performance Monitor and Windows	254
	Lab 5.3: Work with Unix/Linux Networking	255
	Review Questions	256
	Answers to Review Questions	260
Chapter 6	Securing the Network and Environment	261
	Understanding Physical and Network Security	262
	Implementing Access Control	262
	Understanding Social Engineering	270
	Scanning the Environment	272
	Understanding Business Continuity Planning	281
	Undertaking Business Impact Analysis	281
	Assessing Risk	282
	Developing Policies, Standards, and Guidelines	285
	Implementing Policies	285
	Incorporating Standards	286
	Following Guidelines	287
	Working with Security Standards and ISO 17799	288
	Classifying Information	290
	Public Information	290
	Private Information	292
	Roles in the Security Process	294
	Information Access Controls	295
	Summary	299
	Exam Essentials	301
	Hands-On Lab	303
	Lab 6.1: Test Social Engineering	303
	Review Questions	304
	Answers to Review Questions	308
Chapter 7	Cryptography Basics, Methods, and Standards	311
	An Overview of Cryptography	313
	Understanding Physical Cryptography	314
	Understanding Mathematical Cryptography	316
	Working with Passwords	318
	Understanding Quantum Cryptography	318
	Uncovering the Myth of Unbreakable Codes	319

Understanding Cryptographic Algorithms	321
The Science of Hashing	321
Working with Symmetric Algorithms	323
Working with Asymmetric Algorithms	324
Using Cryptographic Systems	326
Confidentiality	326
Integrity	327
Digital Signatures	328
Authentication	329
Nonrepudiation	330
Access Control	330
Using Public Key Infrastructure	331
Using a Certificate Authority	332
Working with Registration Authorities and Local Registration Authorities	333
Implementing Certificates	335
Understanding Certificate Revocation	336
Implementing Trust Models	337
Preparing for Cryptographic Attacks	341
Understanding Cryptography Standards and Protocols	343
The Origins of Encryption Standards	344
Public-Key Infrastructure X.509/Public-Key Cryptography Standards	348
X.509	348
SSL and TLS	349
Certificate Management Protocols	351
Secure Multipurpose Internet Mail Extensions	351
Secure Electronic Transaction	351
Secure Shell	352
Pretty Good Privacy	354
HTTP Secure	354
Secure HTTP	355
IP Security	355
Tunneling Protocols	356
Federal Information Processing Standard Common Criteria	357
Wireless Transport Layer Security	357
Wired Equivalent Privacy	357
ISO 17799	358
Understanding Key Management and the Key Life Cycle	358
Comparing Centralized and Decentralized Key Generation	359
Storing and Distributing Keys	361
Using Key Escrow	363
Identifying Key Expiration	363
Revoking Keys	364

	Suspending Keys	364
	Recovering and Archiving Keys	365
	Renewing Keys	366
	Destroying Keys	367
	Identifying Key Usage	367
	Summary	368
	Exam Essentials	370
	Hands-On Labs	373
	Lab 7.1: Hash Rules in Windows Server 2003	373
	Lab 7.2: SSL Settings in Windows Server 2003	373
	Lab 7.3: Encrypting a File System in Linux	374
	Lab 7.4: Look for Errors in IPSec Performance Statistics	374
	Review Questions	375
	Answers to Review Questions	379
Chapter 8	Security Policies and Procedures	381
	Understanding Business Continuity	383
	Utilities	384
	High Availability	385
	Disaster Recovery	391
	Reinforcing Vendor Support	404
	Service-Level Agreements	404
	Code Escrow Agreements	406
	Generating Policies and Procedures	406
	Human Resource Policies	406
	Business Policies	410
	Certificate Policies	412
	Incident-Response Policies	413
	Enforcing Privilege Management	414
	User and Group Role Management	415
	Privilege Escalation	416
	Single Sign-On Initiatives	416
	Privilege Decision Making	418
	Auditing	418
	Access Control	422
	Summary	424
	Exam Essentials	425
	Hands-On Labs	427
	Lab 8.1: Use Automated System Recovery in Windows Server 2003	427
	Lab 8.2: Create a Rescue Disk in Linux	427
	Lab 8.3: Create a Backup with SuSE Linux	428
	Review Questions	429
	Answers to Review Questions	433

Chapter 9	Security Administration	435
	Understanding Security Management	436
	Drafting Best Practices and Documentation	436
	Simplifying Security Administration	444
	Understanding Security Awareness and Education	446
	Using Communication and Awareness	447
	Providing Education	447
	Staying on Top of Security	449
	Websites	451
	Trade Publications	452
	Regulating Privacy and Security	454
	The Health Insurance Portability and Accountability Act	454
	The Gramm-Leach-Bliley Act of 1999	454
	The Computer Fraud and Abuse Act	455
	The Family Educational Rights and Privacy Act	455
	The Computer Security Act of 1987	456
	The Cyberspace Electronic Security Act	456
	The Cyber Security Enhancement Act	456
	The Patriot Act	457
	Familiarizing Yourself with International Efforts	457
	Summary	457
	Exam Essentials	458
	Hands-On Labs	459
	Lab 9.1: Configure Windows Automatic Updates	459
	Lab 9.2: Run the Microsoft Baseline Security Analyzer	459
	Review Questions	461
	Answers to Review Questions	465
Appendix A	Security Administrator's Troubleshooting Guide	467
	Getting Started	469
	Access Control Issues	471
	Accountability Concerns	471
	Auditing	472
	Authentication Schemes	473
	Authentication Factors	473
	Mutual Authentication	475
	Authentication Protection	475
	Backup Management	476
	Baselining Security	476
	Certificate Management	477
	Communications Security	478
	Dial-Up	480
	Remote Control/Remote Shell	480
	Virtual Private Networks	480
	Directory Services Protection	481

Disaster Planning	482
Documenting Your Environment	483
E-Mail Issues	483
File-Sharing Basics	484
Working with IDSs and Honey Pots	485
Incident Handling	486
Internet Common Sense	486
Key Management Conventions	488
Preventing Common Malicious Events	489
Antivirus Protection	492
Making Stronger Passwords	493
Managing Personnel	495
Keeping Physical Security Meaningful	495
Securing the Infrastructure	497
Working with Security Zones	499
Social Engineering Risks	500
System Hardening Basics	500
Securing the Wireless Environment	502

Appendix B Workbook Exercises 505

Lab B.1: Change to WPA Security in Windows XP	508
Lab B.2: Turn on the Firewall in Windows XP: Method One	509
Lab B.3: Turn on the Firewall in Windows XP: Method Two	510
Lab B.4: Create a Baseline for Internet Access	511
Lab B.5: Turn on a Screensaver Password for Windows XP	512
Lab B.6: Look for Security Events within Windows XP	512
Lab B.7: Identify User Accounts with Administrator Access in Windows XP	512
Lab B.8: Turn on a Screensaver Password for openSUSE	513
Lab B.9: Change a Password in Linux	514
Lab B.10: Find SUID and SGID Files in Linux	514
Lab B.11: Change ACLs on All Files in a Linux Directory	515
Lab B.12: Change Permissions on All Files in a Linux Directory	515
Lab B.13: Change the Default Permissions for all Newly Created Files in Linux	516
Lab B.14: View all Linux Logins	516
Lab B.15: Change the Group Associated with Files	517
Lab B.16: View Failed Login Attempts	518
Lab B.17: Hide a Linux File	518
Lab B.18: Hide and Access a Windows Share	519
Lab B.19: Encrypt a Windows File	519
Lab B.20: Count the Number of Running Linux Processes	520
Lab B.21: Display the Security Tab in Windows XP	520
Lab B.22: View Effective Permissions in Windows XP	521

	Lab B.23: Turn the Guest Account Off	521
	Lab B.24: View Internet Explorer Security Settings	522
	Lab B.25: Change Internet Explorer Pop-up Blocker Settings	522
	Lab B.26: Prevent a Folder from Being Shared	523
	Lab B.27: Enable openSUSE Firewall	523
	Lab B.28: Configure openSUSE Local Security	524
	Lab B.29: Set the Defaults for New Users	524
	Lab B.30: View Logged Warnings in openSUSE	525
	Lab B.31: Configure AppArmor	525
	Lab B.32: View AppArmor Reports	526
	Lab B.33: Configure openSUSE as a Kerberos Client	526
	Lab B.34: Configure openSUSE as an LDAP Client	527
	Lab B.35: Turn Off IPv6 in openSUSE	527
	Lab B.36: Turn On Folder Encryption with cipher	528
	Lab B.37: Change the Minimum Password Age	528
	Lab B.38: Compare Your System to a Security Template	529
	Lab B.39: Clear Private Data in Internet Explorer	530
	Lab B.40: Clear Private Data in Firefox	531
	Lab B.41: Configure SELinux in Fedora	531
	Lab B.42: Limit Cookies to First Party	531
	Lab B.43: Configure the Phishing Filter	532
	Lab B.44: Add a Legal Notice	532
	Lab B.45: Configure Windows XP Startup	533
	Lab B.46: Run a Remote Desktop	534
	Lab B.47: Secure the Account Database	535
	Lab B.48: Create a Restore Point	536
	Lab B.49: Return to a Restore Point	537
	Lab B.50: Boot to a Good Configuration	537
Appendix	C Security+ Acronym List	539
Appendix	D About the Companion CD	545
	What You'll Find on the CD	546
	Sybex Test Engine	546
	PDF of the Book	546
	Adobe Reader	547
	Electronic Flashcards	547
	System Requirements	547
	Using the CD	547
	Troubleshooting	548
	Customer Care	548
Glossary		549
<i>Index</i>		595