

Contents

<i>Introduction</i>		<i>xv</i>
<i>Assessment Test</i>		<i>xxix</i>
Chapter 1	General Security Concepts	1
	Understanding Information Security	4
	Securing the Physical Environment	5
	Examining Operational Security	7
	Working with Management and Policies	9
	Understanding the Goals of Information Security	13
	Comprehending the Security Process	14
	Appreciating Antivirus Software	14
	Implementing Access Control	14
	Understanding Authentication	16
	Understanding Networking Services and Protocols	22
	Distinguishing Between Security Topologies	24
	Setting Design Goals	25
	Creating Security Zones	27
	Working with Newer Technologies	31
	Business Concerns to Be Aware Of	34
	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	52
	Types of Access Attacks	53
	Recognizing Modification and Repudiation Attacks	55
	Identifying Denial-of-Service (DoS) and Distributed DoS (DDoS) Attacks	55
	Recognizing Common Attacks	57
	Back Door Attacks	57
	Spoofing Attacks	58
	Man-in-the-Middle Attacks	59
	Replay Attacks	60
	Password-Guessing Attacks	61

viii Contents

Identifying TCP/IP Security Concerns	61
Working with the TCP/IP Protocol Suite	63
Encapsulation	66
Working with Protocols and Services	67
Recognizing TCP/IP Attacks	70
Understanding Software Exploitation	76
Surviving Malicious Code	78
Viruses	78
Trojan Horses	85
Logic Bombs	85
Worms	86
Antivirus Software	87
Understanding Social Engineering	88
An Introduction to Auditing Processes and Files	90
Summary	91
Exam Essentials	92
Hands-On Labs	95
Lab 2.1: Identify Running Processes on a Windows-Based Machine	95
Lab 2.2: Identify Running Processes on a Linux-Based Machine	95
Review Questions	97
Answers to Review Questions	101
Chapter 3 Infrastructure and Connectivity	103
Understanding Infrastructure Security	105
Working with Hardware Components	106
Working with Software Components	108
Understanding the Different Network Infrastructure Devices	109
Firewalls	109
Hubs	114
Routers	114
Switches	116
Wireless Access Points	117
Modems	119
Remote Access Services	119
Telecom/PBX Systems	120
Virtual Private Networks	122
Monitoring and Diagnosing Networks	123
Network Monitors	123
Securing Workstations and Servers	125
Understanding Mobile Devices	127

Understanding Remote Access	128
Using the Point-to-Point Protocol	128
Tunneling Protocols	129
802.1x Wireless Protocols	130
RADIUS	130
TACACS/+	131
Securing Internet Connections	132
Working with Ports and Sockets	132
Working with E-mail	133
Working with the Web	134
Working with the File Transfer Protocol	139
Understanding SNMP and	
Other TCP/IP Protocols	141
The Basics of Cabling, Wires, and Communications	142
Coax	142
Unshielded Twisted Pair and Shielded Twisted Pair	146
Fiber Optic	147
Infrared	148
Radio Frequencies	148
Microwave Systems	149
Employing Removable Media	151
Tape	151
CD-R	152
Hard Drives	153
Diskettes	153
Flash Cards	153
Smart Cards	154
Summary	154
Exam Essentials	156
Hands-On Labs	157
Lab 3.1: Examine the Windows Routing Table	157
Lab 3.2: Examine the Linux Routing Table	157
Review Questions	158
Answers to Review Questions	162
Chapter 4	
Monitoring Activity and Intrusion Detection	165
Monitoring the Network	167
Recognizing the Different Types of Network Traffic	168
Monitoring Network Systems	173
Understanding Intrusion Detection Systems	174
Working with a Network-Based IDS	178

x Contents

Working with a Host-Based IDS	183
Utilizing Honey Pots	184
Understanding Incident Response	186
Working with Wireless Systems	191
Wireless Transport Layer Security	191
IEEE 802.11x Wireless Protocols	192
WEP/WAP	192
Wireless Vulnerabilities to Know	193
Understanding Instant Messaging's Features	194
IM Vulnerabilities	195
Controlling Privacy	195
Working with 8.3 File Naming	195
Understanding Packet Sniffing	196
Understanding Signal Analysis and Intelligence	197
Footprinting	197
Scanning	198
Summary	198
Exam Essentials	199
Hands-On Labs	201
Lab 4.1: View the Active TCP and UDP Ports	201
Lab 4.2: Run Windows Network Monitor	201
Lab 4.3: Install snort in Linux	202
Lab 4.4: Make File Extensions Visible in Windows XP	202
Lab 4.5: Monitor Network Traffic in Linux	202
Review Questions	204
Answers to Review Questions	208
Chapter 5	Implementing and Maintaining a Secure Network 211
Overview of Network Security Threats	213
Defining Security Baselines	215
Hardening the OS and NOS	217
Configuring Network Protocols	218
Hardening Microsoft Windows 2000	220
Hardening Microsoft Windows XP	222
Hardening Windows Server 2003	222
Hardening Unix/Linux	223
Hardening Novell NetWare	224
Hardening Apple Macintosh	225
Hardening Filesystems	225
Updating Your Operating System	228
Hardening Network Devices	229
Updating Network Devices	230
Configuring Routers and Firewalls	230

Hardening Applications	231
Hardening Web Servers	232
Hardening E-Mail Servers	233
Hardening FTP Servers	234
Hardening DNS Servers	234
Hardening NNTP Servers	235
Hardening File and Print Servers and Services	236
Hardening DHCP Services	237
Working with Data Repositories	238
Summary	241
Exam Essentials	243
Hands-On Labs	244
Lab 5.1: Install OpenLDAP on a SuSE Server	244
Lab 5.2: Work with Performance Monitor and Windows	244
Lab 5.3: Work with Unix/Linux Networking	245
Lab 5.4: Install and Configure the E-mail Service on a SuSE Server	245
Review Questions	246
Answers to Review Questions	250
Chapter 6	Securing the Network and Environment
	253
Understanding Physical and Network Security	254
Implementing Access Control	254
Understanding Social Engineering	261
Scanning the Environment	264
Understanding Business Continuity Planning	271
Undertaking Business Impact Analysis	272
Assessing Risk	273
Developing Policies, Standards, and Guidelines	275
Implementing Policies	276
Incorporating Standards	277
Following Guidelines	278
Working with Security Standards and ISO 17799	279
Classifying Information	280
Public Information	281
Private Information	282
Roles in the Security Process	284
Information Access Controls	285
Summary	289
Exam Essentials	291
Hands-On Lab	293
Lab 6.1: Test Social Engineering	293
Review Questions	294
Answers to Review Questions	298

Chapter 7	Cryptography Basics, Methods, and Standards	301
	An Overview of Cryptography	303
	Understanding Physical Cryptography	304
	Understanding Mathematical Cryptography	306
	Understanding Quantum Cryptography	308
	Uncovering the Myth of Unbreakable Codes	309
	Understanding Cryptographic Algorithms	310
	The Science of Hashing	310
	Working with Symmetric Algorithms	312
	Working with Asymmetric Algorithms	313
	Using Cryptographic Systems	315
	Confidentiality	315
	Integrity	315
	Authentication	318
	Nonrepudiation	319
	Access Control	319
	Using Public Key Infrastructure	320
	Using a Certificate Authority	321
	Working with Registration Authorities and Local Registration Authorities	322
	Implementing Certificates	324
	Understanding Certificate Revocation	325
	Implementing Trust Models	326
	Preparing for Cryptographic Attacks	330
	Understanding Cryptography Standards and Protocols	332
	The Origins of Encryption Standards	332
	PKIX/PKCS	336
	X.509	337
	SSL and TLS	338
	CMP	339
	S/MIME	340
	SET	340
	SSH	340
	PGP	343
	HTTPS	343
	S-HTTP	344
	IPSec	344
	FIPS	344
	Common Criteria	345
	WTLS	345
	WEP	345
	ISO 17799	345

Understanding Key Management and the Key Life Cycle	346
Comparing Centralized and Decentralized Key Generation	346
Storing and Distributing Keys	348
Using Key Escrow	350
Key Expiration	351
Revoking Keys	351
Suspending Keys	352
Recovering and Archiving Keys	352
Renewing Keys	354
Destroying Keys	355
Key Usage	355
Summary	356
Exam Essentials	358
Hands-On Labs	361
Lab 7.1: Hash Rules in Windows Server 2003	361
Lab 7.2: SSL Settings in Windows Server 2003	361
Lab 7.3: Encrypting a File System in Linux	362
Lab 7.4: Look for Errors in IPSec Performance Statistics	362
Review Questions	363
Answers to Review Questions	367
Chapter 8	
Security Policies and Procedures	369
Understanding Business Continuity	371
Utilities	371
High Availability	372
Disaster Recovery	378
Reinforcing Vendor Support	390
Service-Level Agreements (SLAs)	390
Code Escrow	392
Generating Policies and Procedures	393
Human Resource Policies	393
Business Policies	397
Certificate Policies	398
Incident-Response Policies	400
Enforcing Privilege Management	401
User and Group Role Management	401
Privilege Escalation	403
Single Sign-On	403
Privilege Decision Making	404
Auditing	405
Access Control	407
Summary	408
Exam Essentials	409

xiv Contents

Hands-On Labs	411
Lab 8.1: Use Automated System Recovery in Windows Server 2003	411
Lab 8.2: Create a Rescue Disk in Linux	411
Lab 8.3: Create a Backup with SuSE Linux	411
Review Questions	413
Answers to Review Questions	417
Chapter 9 Security Management	419
Understanding Computer Forensics	420
Methodology of a Forensic Investigation	421
Enforcing the Chain of Custody	423
Preserving Evidence	424
Collecting Evidence	425
Understanding Security Management	426
Drafting Best Practices and Documentation	426
Understanding Security Awareness and Education	433
Using Communication and Awareness	433
Providing Education	433
Staying on Top of Security	436
Websites	437
Trade Publications	438
Regulating Privacy and Security	440
Health Insurance Portability and Accountability Act	440
Gramm-Leach-Bliley Act of 1999	440
Computer Fraud and Abuse Act	441
Family Educational Rights and Privacy Act	441
Computer Security Act of 1987	442
Cyberspace Electronic Security Act	442
Cyber Security Enhancement Act	442
Patriot Act	442
Familiarizing Yourself with International Efforts	443
Summary	444
Exam Essentials	445
Hands-On Labs	447
Lab 9.1: Configure Windows Automatic Updates	447
Lab 9.2: Configure Linux Automatic Updates	447
Review Questions	448
Answers to Review Questions	452
Glossary	455
<i>Index</i>	495