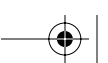


Contents at a Glance

<i>Introduction</i>		<i>xiii</i>
Chapter 1	General Security Concepts	1
Chapter 2	Communication Security	37
Chapter 3	Infrastructure Security	71
Chapter 4	Basics of Cryptography	117
Chapter 5	Operational/Organizational Security	147
<i>Index</i>		<i>181</i>

COPYRIGHTED MATERIAL



Contents

Introduction

xiii

Chapter 1	General Security Concepts	1
1.1	Identifying Access Control Models	3
	Critical Information	3
	Role-Based Access Control (RBAC)	6
	Exam Essentials	6
1.2	Identifying Authentication Methods	7
	Critical Information	7
	Exam Essentials	15
1.3	Identifying Non-Essential Services	15
	Critical Information	16
	Exam Essentials	17
1.4	Identifying Attack Methods	18
	Critical Information	18
	Exam Essentials	28
1.5	Identifying Malicious Code	29
	Critical Information	29
	Exam Essentials	30
1.6	Understanding Social Engineering	31
	Critical Information	31
	Exam Essentials	32
1.7	Understanding Auditing	32
	Critical Information	33
	Exam Essentials	33
	Review Questions	34
	Answers to Review Questions	36
Chapter 2	Communication Security	37
2.1	Remote Access Technologies	39
	Critical Information	40
	Exam Essentials	47
2.2	E-mail Security	48
	Critical Information	48
	Exam Essentials	53
2.3	Internet Security	54
	Critical Information	54
	Exam Essentials	59

x Contents

	2.4 Directory Security	60
	Critical Information	60
	Exam Essentials	61
	2.5 File Transfer Protocols	61
	Critical Information	62
	Exam Essentials	63
	2.6 Wireless	64
	Critical Information	64
	Exam Essentials	66
	Review Questions	68
	Answers to Review Questions	70
Chapter 3	Infrastructure Security	71
	3.1 Security Devices	74
	Critical Information	74
	Exam Essentials	82
	3.2 Media Security	82
	Critical Information	82
	Exam Essentials	88
	3.3 Security Topologies	89
	Critical Information	89
	Exam Essentials	94
	3.4 Intrusion Detection	95
	Critical Information	95
	Active Detection and Passive Detection	97
	Exam Essentials	102
	3.5 Environment Hardening	103
	Critical Information	103
	Exam Essentials	111
	Review Questions	113
	Answers to Review Questions	115
Chapter 4	Basics of Cryptography	117
	4.1 Cryptographic Algorithms	119
	Critical Information	119
	Exam Essentials	124
	4.2 Cryptography Security Concepts	125
	Critical Information	125
	Exam Essentials	128
	4.3 Public Key Infrastructure	129
	Critical Information	129
	Exam Essentials	134
	4.4 Cryptographic Standards and Protocols	135

	4.5 Key Management and Certificate Life Cycles	136
	Critical Information	136
	Exam Essentials	141
	Review Questions	144
	Answers to Review Questions	146
Chapter 5	Operational/Organizational Security	147
	5.1 Physical Security	150
	Critical Information	150
	Exam Essentials	155
	5.2 Disaster Recovery	156
	Critical Information	156
	Exam Essentials	158
	5.3 Business Continuity	159
	Critical Information	159
	Exam Essentials	162
	5.4 Security Policy Issues	163
	Critical Information	163
	Exam Essentials	166
	5.5 Privilege Management	167
	Critical Information	167
	Exam Essentials	169
	5.6 Forensics	170
	Critical Information	170
	Exam Essentials	171
	5.7 Risk Identification	171
	Critical Information	171
	Exam Essentials	173
	5.8 Security Training	173
	Critical Information	173
	Exam Essentials	174
	5.9 Security Documentation	175
	Critical Information	175
	Exam Essentials	177
	Review Questions	178
	Answers to Review Questions	180
<i>Index</i>		181