

Contents

Introduction

xxiii

Phase 1	The Grunt Work of Security	1
	Task 1.1: Performing an Initial Risk Assessment	2
	Scenario	3
	Scope of Task	3
	Procedure	3
	Criteria for Completion	8
	Task 1.2: Determining Which Security Policy Is Most Important	8
	Scenario	8
	Scope of Task	8
	Procedure	9
	Criteria for Completion	12
	Task 1.3: Establishing a User-Awareness Program	12
	Scenario	13
	Scope of Task	13
	Procedure	13
	Criteria for Completion	16
	Task 1.4: Reviewing a Physical-Security Checklist	16
	Scenario	16
	Scope of Task	17
	Procedure	17
	Criteria for Completion	19
	Task 1.5: Understanding the Value of Documents	19
	Scenario	19
	Scope of Task	20
	Procedure	20
	Criteria for Completion	22
Phase 2	Hardening Systems	23
	Task 2.1: Managing Services	24
	Scenario	25
	Scope of Task	25
	Procedure	26
	Criteria for Completion	38

Task 2.2: Managing Ports	38
Scenario	38
Scope of Task	39
Procedure	39
Criteria for Completion	48
Task 2.3: Patching the Operating System	49
Scenario	49
Scope of Task	49
Procedure	49
Criteria for Completion	64
Task 2.4: Security Templates	64
Scenario	64
Scope of Task	65
Procedure	65
Criteria for Completion	74
Task 2.5: Securing Autoruns	74
Scenario	74
Scope of Task	74
Procedure	75
Criteria for Completion	84
Task 2.6: Securing Hardware Devices	84
Scenario	84
Scope of Task	84
Procedure	85
Criteria for Completion	94
Task 2.7: Virtualization	95
Scenario	95
Scope of Task	95
Procedure	96
Criteria for Completion	103

Phase 3 Malicious Software 105

Task 3.1: Installing, Updating, and Running Antivirus Software	106
Scenario	106
Scope of Task	107
Procedure	107
Criteria for Completion	112

Task 3.2: Using a Rootkit Checker	112
Scenario	113
Scope of Task	113
Procedure	113
Criteria for Completion	118
Task 3.3: Using Adware Checker	118
Scenario	119
Scope of Task	119
Procedure	119
Criteria for Completion	123
Task 3.4: Using Spyware Checker	123
Scenario	123
Scope of Task	123
Procedure	124
Criteria for Completion	127
Task 3.5: Malicious Software Removal Tool	127
Scenario	127
Scope of Task	127
Procedure	128
Criteria for Completion	130
Task 3.6: McAfee Site Advisor	130
Scenario	130
Scope of Task	130
Procedure	131
Criteria for Completion	133
Task 3.7: ARP Poisoning with Cain & Abel	133
Scenario	133
Scope of Task	134
Procedure	134
Criteria for Completion	140
Phase 4	Secure Storage
	141
Task 4.1: The Encrypting File System	142
Scenario	143
Scope of Task	143
Procedure	143
Criteria for Completion	157

Task 4.2: EFS Data Recovery	157
Scenario	157
Scope of Task	157
Procedure	158
Criteria for Completion	161
Task 4.3: Implementing Syskey	161
Scenario	162
Scope of Task	162
Procedure	162
Criteria for Completion	164
Task 4.4: Converting FAT to NTFS	165
Scenario	165
Scope of Task	165
Procedure	166
Criteria for Completion	174
Task 4.5: Implementing Disk Fault Tolerance with RAID	174
Scenario	175
Scope of Task	175
Procedure	175
Criteria for Completion	180
Task 4.6: Backing Up Data	180
Scenario	180
Scope of Task	181
Procedure	181
Criteria for Completion	188
Task 4.7: Restoring Data from a Backup	188
Scenario	188
Scope of Task	189
Procedure	189
Criteria for Completion	193
Task 4.8: Securing Shares	193
Scenario	194
Scope of Task	194
Procedure	194
Criteria for Completion	204
Task 4.9: BitLocker Drive Encryption	204
Scenario	205
Scope of Task	205

	Procedure	206
	Criteria for Completion	217
Phase 5	Managing User Accounts	219
	Task 5.1: Creating User Accounts	220
	Scenario	220
	Scope of Task	220
	Procedure	221
	Criteria for Completion	226
	Task 5.2: Implementing the Password Policy	226
	Scenario	227
	Scope of Task	227
	Procedure	227
	Criteria for Completion	231
	Task 5.3: Auditing Logons	231
	Scenario	232
	Scope of Task	232
	Procedure	233
	Criteria for Completion	238
	Task 5.4: Securing the Default User Accounts	239
	Scenario	239
	Scope of Task	239
	Procedure	240
	Criteria for Completion	246
	Task 5.5: Implementing a Deny Group	247
	Scenario	247
	Scope of Task	247
	Procedure	247
	Criteria for Completion	252
Phase 6	Network Security	253
	Task 6.1: Deploying IPSec	255
	Scenario	255
	Scope of Task	255
	Procedure	256
	Criteria for Completion	259
	Task 6.2: Configuring the VPN Server	259
	Scenario	260
	Scope of Task	260

	Procedure	261	
	Criteria for Completion	266	
	Task 6.3: Configuring the VPN Client	266	
	Scenario	266	
	Scope of Task	266	
	Procedure	266	
	Criteria for Completion	270	
	Task 6.4: Implementing Secure Remote Administration	270	
	Scenario	271	
	Scope of Task	271	
	Procedure	271	
	Criteria for Completion	277	
	Task 6.5: Secure Administration Using Run As	278	
	Scenario	279	
	Scope of Task	279	
	Procedure	279	
	Criteria for Completion	284	
	Task 6.6: Configuring a Packet Filter	284	
	Scenario	284	
	Scope of Task	284	
	Procedure	285	
	Criteria for Completion	289	
	Task 6.7: Implementing 802.11 Wireless Security	289	
	Scenario	290	
	Scope of Task	290	
	Procedure	290	
	Criteria for Completion	300	
	Task 6.8: Implementing an IPSec VPN Using AES	300	
	Scenario	300	
	Scope of Task	301	
	Procedure	301	
	Criteria for Completion	317	
Phase	7	Securing Internet Activity	319
		Task 7.1: Configuring Internet Access	320
		Scenario	321
		Scope of Task	321

Procedure	321
Criteria for Completion	324
Task 7.2: Using Internet Explorer Security Zones	324
Scenario	324
Scope of Task	324
Procedure	324
Criteria for Completion	328
Task 7.3: Configuring IE for Secure Use of Cookies	328
Scenario	328
Scope of Task	328
Procedure	329
Criteria for Completion	330
Task 7.4: Using Internet Connection Sharing	330
Scenario	330
Scope of Task	330
Procedure	331
Criteria for Completion	334
Task 7.5: Securing E-mail	334
Scenario	335
Scope of Task	335
Procedure	335
Criteria for Completion	339
Task 7.6: Spam Management	339
Scenario	339
Scope of Task	340
Procedure	340
Criteria for Completion	343
Task 7.7: Installing and Using a Digital Certificate	344
Scenario	344
Scope of Task	344
Procedure	344
Criteria for Completion	347
Task 7.8: Certificate Backup and Management	348
Scenario	348
Scope of Task	348
Procedure	348
Criteria for Completion	353

	Task 7.9: Performing Secure File Exchange	353
	Scenario	353
	Scope of Task	353
	Procedure	353
	Criteria for Completion	357
	Task 7.10: Validating Downloads and Checking the Hash	357
	Scenario	358
	Scope of Task	358
	Procedure	358
	Criteria for Completion	360
	Task 7.11: Logging and Recording Internet Activity	361
	Scenario	361
	Scope of Task	361
	Procedure	361
	Criteria for Completion	365
Phase 8	Security Testing	367
	Task 8.1: Penetration Testing with Nessus	368
	Scenario	368
	Scope of Task	369
	Procedure	369
	Criteria for Completion	373
	Task 8.2: Penetration Testing with Retina	374
	Scenario	374
	Scope of Task	374
	Procedure	374
	Criteria for Completion	378
	Task 8.3: Performing Assessments with MBSA	379
	Scenario	379
	Scope of Task	379
	Procedure	379
	Criteria for Completion	382
	Task 8.4: Performing Security Assessments with HFNetChk	382
	Scenario	383
	Scope of Task	383
	Procedure	383
	Criteria for Completion	385

Task 8.5: Performing Internet Vulnerability Profiling	385
Scenario	385
Scope of Task	386
Procedure	386
Criteria for Completion	390
Task 8.6: Tracking Hostile IPs	390
Scenario	390
Scope of Task	390
Procedure	390
Criteria for Completion	393
Task 8.7: Investigating Netcat	393
Scenario	393
Scope of Task	394
Procedure	394
Criteria for Completion	397

Phase 9 Investigating Incidents 399

Task 9.1: Configuring an Audit Policy for Object Access	401
Scenario	401
Scope of Task	401
Procedure	402
Criteria for Completion	410
Task 9.2: Reviewing the Audit Logs	411
Scenario	411
Scope of Task	411
Procedure	412
Criteria for Completion	420
Task 9.3: Forcing a Memory Dump	420
Scenario	420
Scope of Task	420
Procedure	421
Criteria for Completion	428
Task 9.4: Capturing Packets with the Packet Analyzer: Wireshark	428
Scenario	430
Scope of Task	430
Procedure	431
Criteria for Completion	438

	Task 9.5: Recovering Previous Versions of Files	438	
	Scenario	439	
	Scope of Task	439	
	Procedure	440	
	Criteria for Completion	452	
Phase	10	Security Troubleshooting	453
	Task 10.1: Booting into Safe Mode	455	
	Scenario	455	
	Scope of Task	455	
	Procedure	456	
	Criteria for Completion	459	
	Task 10.2: Implementing Last Known Good Configuration	459	
	Scenario	459	
	Scope of Task	460	
	Procedure	460	
	Criteria for Completion	462	
	Task 10.3: Using System Restore	462	
	Scenario	463	
	Scope of Task	463	
	Procedure	464	
	Criteria for Completion	470	
	Task 10.4: Sanitizing Media	470	
	Scenario	470	
	Scope of Task	471	
	Procedure	471	
	Criteria for Completion	475	
	Task 10.5: Implementing a Host-Based Intrusion Detection System	475	
	Scenario	476	
	Scope of Task	476	
	Procedure	477	
	Criteria for Completion	486	
	<i>Index</i>	487	