Contents

Introduction *xix*

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 9
Procedure 9
Criteria for Completion 12
Task 1.3: Establishing a User Awareness Program 13
Scenario 13
Scope of Task 13
Procedure 14
Criteria for Completion 16
Task 1.4: Reviewing a Physical Security Checklist 16
Scenario 16
Scope of Task 16
Procedure 17
Criteria for Completion 19
Task 1.5: Understanding the Value of Documents 19
Scenario 19
Scope of Task 19
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 39
Task 2.2: Managing Ports 39
Scenario 39
Scope of Task 40
Procedure 40
Criteria for Completion 50

Task 2.3: Patching the Operating System 51
Scenario 51
Scope of Task 51
Procedure 51
Criteria for Completion 67
Task 2.4: Security Templates 67
Scenario 67
Scope of Task 68
Procedure 68
Criteria for Completion 77
Task 2.5: Securing Autoruns 77
Scenario 77
Scope of Task 78
Procedure 78
Criteria for Completion 87

Phase 3 Protecting Against Malware 89

Task 3.1: Installing, Updating, and Running Antivirus Software 90
Scenario 91
Scope of Task 91
Procedure 91
Criteria for Completion 96
Task 3.2: Using a Rootkit Checker 96
Scenario 97
Scope of Task 97
Procedure 97
Criteria for Completion 102
Task 3.3: Using Adware Checker 102
Scenario 102
Scope of Task 103
Procedure 103
Criteria for Completion 106
Task 3.4: Using Spyware Checker 106
Scenario 106
Scope of Task 107
Procedure 107
Criteria for Completion 110

Phase 4 Secure Storage 111

Task 4.1: The Encrypting File System 112
Scenario 112
Scope of Task 113

Procedure 113
Criteria for Completion 127
Task 4.2: EFS Data Recovery 127
Scenario 127
Scope of Task 127
Procedure 128
Criteria for Completion 131
Task 4.3: Implementing Syskey 131
Scenario 132
Scope of Task 132
Procedure 132
Criteria for Completion 134
Task 4.4: Converting FAT to NTFS 134
Scenario 135
Scope of Task 135
Procedure 136
Criteria for Completion 145
Task 4.5: Implementing Disk Fault Tolerance with RAID 145
Scenario 146
Scope of Task 146
Procedure 146
Criteria for Completion 151
Task 4.6: Backing Up Data 151
Scenario 152
Scope of Task 152
Procedure 152
Criteria for Completion 160
Task 4.7: Restoring Data from a Backup 161
Scenario 161
Scope of Task 161
Procedure 162
Criteria for Completion 166
Task 4.8: Securing Shares 167
Scenario 167
Scope of Task 167
Procedure 168
Criteria for Completion 177

Phase 5 Managing User Accounts 179

Task 5.1: Creating User Accounts 180
Scenario 180
Scope of Task 181

Procedure 181
Criteria for Completion 187
Task 5.2: Implementing the Password Policy 187
Scenario 187
Scope of Task 187
Procedure 188
Criteria for Completion 192
Task 5.3: Auditing Logons 192
Scenario 192
Scope of Task 192
Procedure 193
Criteria for Completion 199
Task 5.4: Securing the Default User Accounts 200
Scenario 200
Scope of Task 200
Procedure 201
Criteria for Completion 208
Task 5.5: Implementing a Deny Group 208
Scenario 208
Scope of Task 208
Procedure 209
Criteria for Completion 214

Phase 6 Network Security 215

Task 6.1: Deploying IPSec 217
Scenario 217
Scope of Task 217
Procedure 218
Criteria for Completion 221
Task 6.2: Configuring the VPN Server 221
Scenario 222
Scope of Task 222
Procedure 223
Criteria for Completion 228
Task 6.3: Configuring the VPN Client 228
Scenario 228
Scope of Task 228
Procedure 229
Criteria for Completion 233
Task 6.4: Implementing Secure Remote Administration 233
Scenario 233
Scope of Task 233

Procedure 234
Criteria for Completion 240
Task 6.5: Secure Administration Using Run As 241
Scenario 242
Scope of Task 242
Procedure 242
Criteria for Completion 247
Task 6.6: Configuring a Packet Filter 247
Scenario 247
Scope of Task 248
Procedure 248
Criteria for Completion 252
Task 6.7: Implementing 802.11 Wireless Security 252
Scenario 253
Scope of Task 253
Procedure 253
Criteria for Completion 264

Phase 7 Securing Internet Activity 265

Task 7.1: Configuring Internet Access 266
Scenario 267
Scope of Task 267
Procedure 267
Criteria for Completion 270
Task 7.2: Using Internet Explorer Security Zones 270
Scenario 270
Scope of Task 270
Procedure 271
Criteria for Completion 274
Task 7.3: Configuring IE for Secure Use of Cookies 274
Scenario 274
Scope of Task 274
Procedure 275
Criteria for Completion 276
Task 7.4: Using Internet Connection Sharing 276
Scenario 276
Scope of Task 276
Procedure 277
Criteria for Completion 280
Task 7.5: Securing E-mail 281
Scenario 281
Scope of Task 281

Procedure 282
Criteria for Completion 285
Task 7.6: Spam Management 286
Scenario 286
Scope of Task 286
Procedure 286
Criteria for Completion 290
Task 7.7: Installing and Using a Digital Certificate 290
Scenario 290
Scope of Task 291
Procedure 291
Criteria for Completion 294
Task 7.8: Certificate Backup and Management 294
Scenario 294
Scope of Task 294
Procedure 295
Criteria for Completion 298
Task 7.9: Performing Secure File Exchange 298
Scenario 298
Scope of Task 299
Procedure 299
Criteria for Completion 303
Task 7.10: Validating Downloads and Checking the Hash 303
Scenario 303
Scope of Task 304
Procedure 304
Criteria for Completion 306

Phase 8 Security Testing 307

Task 8.1: Penetration Testing with Nessus 308
Scenario 308
Scope of Task 309
Procedure 309
Criteria for Completion 313
Task 8.2: Penetration Testing with Retina 314
Scenario 314
Scope of Task 314
Procedure 314
Criteria for Completion 319
Task 8.3: Performing Assessments with Microsoft Baseline Security Analyzer 320
Scenario 320
Scope of Task 320

Procedure 320
Criteria for Completion 323
Task 8.4: Performing Security Assessments with HFNetChk 323
Scenario 324
Scope of Task 324
Procedure 324
Criteria for Completion 326
Task 8.5: Performing Internet Vulnerability Profiling 326
Scenario 327
Scope of Task 327
Procedure 327
Criteria for Completion 331

Phase 9 Investigating Incidents 333

Task 9.1: Configuring an Audit Policy for Object Access 335
Scenario 335
Scope of Task 335
Procedure 336
Criteria for Completion 345
Task 9.2: Reviewing the Audit Logs 345
Scenario 345
Scope of Task 345
Procedure 346
Criteria for Completion 354
Task 9.3: Forcing a Memory Dump 354
Scenario 354
Scope of Task 354
Procedure 355
Criteria for Completion 362
Task 9.4: Capturing Packets with the Packet Analyzer: Ethereal 362
Scenario 363
Scope of Task 364
Procedure 364
Criteria for Completion 372
Task 9.5: Recovering Previous Versions of Files 372
Scenario 373
Scope of Task 373
Procedure 373
Criteria for Completion 387

Phase 10 Security Troubleshooting 389

Task 10.1: Booting into Safe Mode 391
Scenario 391
Scope of Task 391
Procedure 392
Criteria for Completion 395
Task 10.2: Implementing Last Known Good Configuration 395
Scenario 395
Scope of Task 395
Procedure 396
Criteria for Completion 398
Task 10.3: Using System Restore 398
Scenario 399
Scope of Task 399
Procedure 399
Criteria for Completion 405
Task 10.4: Sanitizing Media 406
Scenario 406
Scope of Task 406
Procedure 407
Criteria for Completion 410

Index *411*