# Contents

*Introduction*  

**Phase 1**  
**The Grunt Work of Security**  

Task 1.1: Performing an Initial Risk Assessment  
- Scenario 3  
- Scope of Task 3  
- Procedure 3  
- Criteria for Completion 8  

Task 1.2: Determining Which Security Policy Is Most Important  
- Scenario 8  
- Scope of Task 8  
- Procedure 9  
- Criteria for Completion 12  

Task 1.3: Establishing a User-Awareness Program  
- Scenario 13  
- Scope of Task 13  
- Procedure 13  
- Criteria for Completion 16  

Task 1.4: Reviewing a Physical-Security Checklist  
- Scenario 16  
- Scope of Task 16  
- Procedure 17  
- Criteria for Completion 19  

Task 1.5: Understanding the Value of Documents  
- Scenario 19  
- Scope of Task 19  
- Procedure 20  
- Criteria for Completion 22  

**Phase 2**  
**Hardening Systems**  

Task 2.1: Managing Services  
- Scenario 25  
- Scope of Task 25  
- Procedure 26  
- Criteria for Completion 39  

Task 2.2: Managing Ports  
- Scenario 39  
- Scope of Task 39  
- Procedure 40  
- Criteria for Completion 49
Task 2.3: Patching the Operating System 50
  Scenario 50
  Scope of Task 50
  Procedure 50
  Criteria for Completion 65
Task 2.4: Security Templates 65
  Scenario 65
  Scope of Task 66
  Procedure 66
  Criteria for Completion 74
Task 2.5: Securing Autoruns 74
  Scenario 74
  Scope of Task 74
  Procedure 75
  Criteria for Completion 83
Task 2.6: Securing Hardware Devices 83
  Scenario 84
  Scope of Task 84
  Procedure 84
  Criteria for Completion 94
Task 2.7: Virtualization 94
  Scenario 94
  Scope of Task 94
  Procedure 95
  Criteria for Completion 102
Task 2.8: Locking the Computer Using an Idle Time-out 102
  Scenario 102
  Scope of Task 102
  Procedure 103
  Criteria for Completion 109

Phase 3 Malicious Software 111
Task 3.1: Installing, Updating, and Running Antivirus Software 112
  Scenario 113
  Scope of Task 113
  Procedure 113
  Criteria for Completion 119
Task 3.2: Using a Rootkit Checker 119
  Scenario 119
  Scope of Task 120
  Procedure 120
  Criteria for Completion 125
Task 3.3: Adware 125
   Scenario 125
   Scope of Task 125
   Procedure 126
   Criteria for Completion 129
Task 3.4: Using a Spyware Checker 129
   Scenario 130
   Scope of Task 130
   Procedure 130
   Criteria for Completion 133
Task 3.5: Malicious Software Removal Tool 133
   Scenario 134
   Scope of Task 134
   Procedure 134
   Criteria for Completion 136
Task 3.6: McAfee Site Advisor 137
   Scenario 137
   Scope of Task 137
   Procedure 137
   Criteria for Completion 140
Task 3.7: ARP Poisoning with Cain & Abel 141
   Scenario 141
   Scope of Task 141
   Procedure 141
   Criteria for Completion 150
Task 3.8: Attacking Authentication with Firesheep 150
   Scenario 150
   Scope of Task 150
   Procedure 151
   Criteria for Completion 153

Phase 4 Secure Storage 155
Task 4.1: The Encrypting File System 156
   Scenario 157
   Scope of Task 157
   Procedure 157
   Criteria for Completion 170
Task 4.2: EFS Data Recovery 170
   Scenario 171
   Scope of Task 171
   Procedure 171
   Criteria for Completion 175
<table>
<thead>
<tr>
<th>Task</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>4.3</td>
<td>Implementing Syskey</td>
<td>175</td>
</tr>
<tr>
<td></td>
<td>Scenario</td>
<td>175</td>
</tr>
<tr>
<td></td>
<td>Scope of Task</td>
<td>176</td>
</tr>
<tr>
<td></td>
<td>Procedure</td>
<td>176</td>
</tr>
<tr>
<td></td>
<td>Criteria for Completion</td>
<td>178</td>
</tr>
<tr>
<td>4.4</td>
<td>Converting FAT to NTFS</td>
<td>178</td>
</tr>
<tr>
<td></td>
<td>Scenario</td>
<td>179</td>
</tr>
<tr>
<td></td>
<td>Scope of Task</td>
<td>179</td>
</tr>
<tr>
<td></td>
<td>Procedure</td>
<td>180</td>
</tr>
<tr>
<td></td>
<td>Criteria for Completion</td>
<td>188</td>
</tr>
<tr>
<td>4.5</td>
<td>Implementing Disk Fault Tolerance with RAID</td>
<td>188</td>
</tr>
<tr>
<td></td>
<td>Scenario</td>
<td>189</td>
</tr>
<tr>
<td></td>
<td>Scope of Task</td>
<td>189</td>
</tr>
<tr>
<td></td>
<td>Procedure</td>
<td>189</td>
</tr>
<tr>
<td></td>
<td>Criteria for Completion</td>
<td>194</td>
</tr>
<tr>
<td>4.6</td>
<td>Backing Up Data</td>
<td>194</td>
</tr>
<tr>
<td></td>
<td>Scenario</td>
<td>194</td>
</tr>
<tr>
<td></td>
<td>Scope of Task</td>
<td>194</td>
</tr>
<tr>
<td></td>
<td>Procedure</td>
<td>195</td>
</tr>
<tr>
<td></td>
<td>Criteria for Completion</td>
<td>203</td>
</tr>
<tr>
<td>4.7</td>
<td>Restoring Data from a Backup</td>
<td>203</td>
</tr>
<tr>
<td></td>
<td>Scenario</td>
<td>203</td>
</tr>
<tr>
<td></td>
<td>Scope of Task</td>
<td>203</td>
</tr>
<tr>
<td></td>
<td>Procedure</td>
<td>204</td>
</tr>
<tr>
<td></td>
<td>Criteria for Completion</td>
<td>208</td>
</tr>
<tr>
<td>4.8</td>
<td>Securing Shares</td>
<td>208</td>
</tr>
<tr>
<td></td>
<td>Scenario</td>
<td>209</td>
</tr>
<tr>
<td></td>
<td>Scope of Task</td>
<td>209</td>
</tr>
<tr>
<td></td>
<td>Procedure</td>
<td>209</td>
</tr>
<tr>
<td></td>
<td>Criteria for Completion</td>
<td>219</td>
</tr>
<tr>
<td>4.9</td>
<td>BitLocker Drive Encryption</td>
<td>219</td>
</tr>
<tr>
<td></td>
<td>Scenario</td>
<td>220</td>
</tr>
<tr>
<td></td>
<td>Scope of Task</td>
<td>220</td>
</tr>
<tr>
<td></td>
<td>Procedure</td>
<td>221</td>
</tr>
<tr>
<td></td>
<td>Criteria for Completion</td>
<td>232</td>
</tr>
<tr>
<td>4.10</td>
<td>Securing Data to Satisfy FIPS 140-2 Using PGP Desktop</td>
<td>232</td>
</tr>
<tr>
<td></td>
<td>Scenario</td>
<td>233</td>
</tr>
<tr>
<td></td>
<td>Scope of Task</td>
<td>233</td>
</tr>
<tr>
<td></td>
<td>Procedure</td>
<td>234</td>
</tr>
<tr>
<td></td>
<td>Criteria for Completion</td>
<td>250</td>
</tr>
</tbody>
</table>
## Phase 5  
### Managing User Accounts  
**Task 5.1: Creating User Accounts**  
- Scenario 252  
- Scope of Task 253  
- Procedure 253  
- Criteria for Completion 259  
**Task 5.2: Implementing the Password Policy**  
- Scenario 259  
- Scope of Task 260  
- Procedure 260  
- Criteria for Completion 263  
**Task 5.3: Auditing Logons**  
- Scenario 264  
- Scope of Task 264  
- Procedure 265  
- Criteria for Completion 271  
**Task 5.4: Securing the Default User Accounts**  
- Scenario 271  
- Scope of Task 272  
- Procedure 272  
- Criteria for Completion 279  
**Task 5.5: Implementing a Deny Group**  
- Scenario 279  
- Scope of Task 279  
- Procedure 280  
- Criteria for Completion 285  

## Phase 6  
### Network Security  
**Task 6.1: Deploying IPSec**  
- Scenario 289  
- Scope of Task 290  
- Procedure 290  
- Criteria for Completion 293  
**Task 6.2: Configuring the VPN Server**  
- Scenario 293  
- Scope of Task 294  
- Procedure 295  
- Criteria for Completion 300  
**Task 6.3: Configuring the VPN Client**  
- Scenario 300  
- Scope of Task 300  
- Procedure 300  
- Criteria for Completion 304
<table>
<thead>
<tr>
<th>Task 6.4: Implementing Secure Remote Administration</th>
<th>304</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scenario</td>
<td>305</td>
</tr>
<tr>
<td>Scope of Task</td>
<td>305</td>
</tr>
<tr>
<td>Procedure</td>
<td>305</td>
</tr>
<tr>
<td>Criteria for Completion</td>
<td>312</td>
</tr>
<tr>
<td>Task 6.5: Secure Administration Using Run As</td>
<td>312</td>
</tr>
<tr>
<td>Scenario</td>
<td>313</td>
</tr>
<tr>
<td>Scope of Task</td>
<td>313</td>
</tr>
<tr>
<td>Procedure</td>
<td>313</td>
</tr>
<tr>
<td>Criteria for Completion</td>
<td>318</td>
</tr>
<tr>
<td>Task 6.6: Configuring a Packet Filter</td>
<td>319</td>
</tr>
<tr>
<td>Scenario</td>
<td>319</td>
</tr>
<tr>
<td>Scope of Task</td>
<td>319</td>
</tr>
<tr>
<td>Procedure</td>
<td>319</td>
</tr>
<tr>
<td>Criteria for Completion</td>
<td>323</td>
</tr>
<tr>
<td>Task 6.7: Implementing 802.11 Wireless Security</td>
<td>323</td>
</tr>
<tr>
<td>Scenario</td>
<td>324</td>
</tr>
<tr>
<td>Scope of Task</td>
<td>324</td>
</tr>
<tr>
<td>Procedure</td>
<td>325</td>
</tr>
<tr>
<td>Criteria for Completion</td>
<td>335</td>
</tr>
<tr>
<td>Task 6.8: Implementing an IPSec VPN Using AES</td>
<td>335</td>
</tr>
<tr>
<td>Scenario</td>
<td>335</td>
</tr>
<tr>
<td>Scope of Task</td>
<td>336</td>
</tr>
<tr>
<td>Procedure</td>
<td>336</td>
</tr>
<tr>
<td>Criteria for Completion</td>
<td>352</td>
</tr>
<tr>
<td>Task 6.9: Implementing a Personal Firewall</td>
<td>352</td>
</tr>
<tr>
<td>Scenario</td>
<td>353</td>
</tr>
<tr>
<td>Scope of Task</td>
<td>353</td>
</tr>
<tr>
<td>Procedure</td>
<td>353</td>
</tr>
<tr>
<td>Criteria for Completion</td>
<td>361</td>
</tr>
</tbody>
</table>

**Phase 7  Securing Internet Activity 363**

| Task 7.1: Configuring Internet Access              | 364 |
| Scenario                                           | 365 |
| Scope of Task                                      | 365 |
| Procedure                                          | 365 |
| Criteria for Completion                            | 367 |
| Task 7.2: Using Internet Explorer Security Zones   | 367 |
| Scenario                                           | 368 |
| Scope of Task                                      | 368 |
| Procedure                                          | 368 |
| Criteria for Completion                            | 371 |
Task 7.3: Configuring IE for Secure Use of Cookies 371
  Scenario 372
  Scope of Task 372
  Procedure 372
  Criteria for Completion 373
Task 7.4: Using Internet Connection Sharing 373
  Scenario 374
  Scope of Task 374
  Procedure 374
  Criteria for Completion 378
Task 7.5: Securing Email 378
  Scenario 378
  Scope of Task 378
  Procedure 379
  Criteria for Completion 382
Task 7.6: Spam Management 382
  Scenario 383
  Scope of Task 383
  Procedure 383
  Criteria for Completion 387
Task 7.7: Installing and Using a Digital Certificate 387
  Scenario 387
  Scope of Task 387
  Procedure 387
  Criteria for Completion 390
Task 7.8: Certificate Backup and Management 391
  Scenario 391
  Scope of Task 391
  Procedure 391
  Criteria for Completion 396
Task 7.9: Performing Secure File Exchange 396
  Scenario 396
  Scope of Task 396
  Procedure 396
  Criteria for Completion 400
Task 7.10: Validating Downloads and Checking the Hash 400
  Scenario 400
  Scope of Task 401
  Procedure 401
  Criteria for Completion 403
Task 7.11: Logging and Recording Internet Activity 403
  Scenario 403
  Scope of Task
Procedure 403
Criteria for Completion 407

Task 7.12: Using HTTPS to Encrypt Web Traffic 407
Scenario 407
Scope of Task 407
Procedure 407
Criteria for Completion 409

Task 7.13: Using Force-TLS to Add Security to Web Browsing 409
Scenario 409
Scope of Task 409
Procedure 410
Criteria for Completion 411

Phase 8

Security Testing 413

Task 8.1: Penetration Testing with Nessus 414
Scenario 415
Scope of Task 415
Procedure 415
Criteria for Completion 419

Task 8.2: Penetration Testing with Retina 419
Scenario 419
Scope of Task 419
Procedure 420
Criteria for Completion 424

Task 8.3: Performing Assessments with MBSA 424
Scenario 425
Scope of Task 425
Procedure 425
Criteria for Completion 428

Task 8.4: Performing Security Assessments with IT Shavlik 428
Scenario 428
Scope of Task 428
Procedure 429
Criteria for Completion 430

Task 8.5: Performing Internet Vulnerability Profiling 430
Scenario 430
Scope of Task 430
Procedure 431
Criteria for Completion 434

Task 8.6: Tracking Hostile IPs 434
Scenario 434
Scope of Task 434
Procedure 435
Criteria for Completion 438
### Task 8.7: Investigating Netcat
- **Scenario**: 438
- **Scope of Task**: 438
- **Procedure**: 438
- **Criteria for Completion**: 441

### Task 8.8: Exploiting Vulnerabilities with Metasploit
- **Scenario**: 442
- **Scope of Task**: 442
- **Procedure**: 442
- **Criteria for Completion**: 446

### Phase 9 Investigating Incidents

#### Task 9.1: Configuring an Audit Policy for Object Access
- **Scenario**: 449
- **Scope of Task**: 449
- **Procedure**: 450
- **Criteria for Completion**: 458

#### Task 9.2: Reviewing the Audit Logs
- **Scenario**: 459
- **Scope of Task**: 459
- **Procedure**: 460
- **Criteria for Completion**: 467

#### Task 9.3: Forcing a Memory Dump
- **Scenario**: 468
- **Scope of Task**: 468
- **Procedure**: 469
- **Criteria for Completion**: 476

#### Task 9.4: Capturing Packets with the Packet Analyzer: Wireshark
- **Scenario**: 476
- **Scope of Task**: 478
- **Procedure**: 478
- **Criteria for Completion**: 486

#### Task 9.5: Recovering Previous Versions of Files
- **Scenario**: 486
- **Scope of Task**: 487
- **Procedure**: 488
- **Criteria for Completion**: 500

#### Task 9.6: Recovering Deleted Content from the File System
- **Scenario**: 501
- **Scope of Task**: 501
- **Procedure**: 502
- **Criteria for Completion**: 516
## Phase 10: Security Troubleshooting

<table>
<thead>
<tr>
<th>Task</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Task 10.1: Booting into Safe Mode</td>
<td>519</td>
</tr>
<tr>
<td>Scenario</td>
<td>519</td>
</tr>
<tr>
<td>Scope of Task</td>
<td>519</td>
</tr>
<tr>
<td>Procedure</td>
<td>520</td>
</tr>
<tr>
<td>Criteria for Completion</td>
<td>523</td>
</tr>
<tr>
<td>Task 10.2: Implementing Last Known Good Configuration</td>
<td>523</td>
</tr>
<tr>
<td>Scenario</td>
<td>523</td>
</tr>
<tr>
<td>Scope of Task</td>
<td>523</td>
</tr>
<tr>
<td>Procedure</td>
<td>524</td>
</tr>
<tr>
<td>Criteria for Completion</td>
<td>526</td>
</tr>
<tr>
<td>Task 10.3: Using System Restore</td>
<td>526</td>
</tr>
<tr>
<td>Scenario</td>
<td>527</td>
</tr>
<tr>
<td>Scope of Task</td>
<td>527</td>
</tr>
<tr>
<td>Procedure</td>
<td>527</td>
</tr>
<tr>
<td>Criteria for Completion</td>
<td>534</td>
</tr>
<tr>
<td>Task 10.4: Sanitizing Media</td>
<td>534</td>
</tr>
<tr>
<td>Scenario</td>
<td>534</td>
</tr>
<tr>
<td>Scope of Task</td>
<td>535</td>
</tr>
<tr>
<td>Procedure</td>
<td>535</td>
</tr>
<tr>
<td>Criteria for Completion</td>
<td>538</td>
</tr>
<tr>
<td>Task 10.5: Implementing a Host-Based Intrusion Detection System</td>
<td>539</td>
</tr>
<tr>
<td>Scenario</td>
<td>540</td>
</tr>
<tr>
<td>Scope of Task</td>
<td>540</td>
</tr>
<tr>
<td>Procedure</td>
<td>541</td>
</tr>
<tr>
<td>Criteria for Completion</td>
<td>550</td>
</tr>
</tbody>
</table>

Index | 551 |