Contents at a Glance

Introduction

Assessment Test

Chapter 1 Configuring, Deploying, and Troubleshooting Security Templates 1
Chapter 2 Configuring Security Based on Computer Roles 45
Chapter 3 Installing, Managing, & Troubleshooting Hotfixes & Service Packs 87
Chapter 4 Configuring IPSec and SMB Signing 131
Chapter 5 Implementing Security for Wireless Networks 175
Chapter 6 Deploying, Managing, and Configuring SSL Certificates 217
Chapter 7 Configuring, Managing, and Troubleshooting Authentication 271
Chapter 8 Configuring and Troubleshooting Virtual Private Network Protocols 321
Chapter 9 Installing, Configuring, and Managing Certificate Authorities 357
Chapter 10 Managing Client-Computer and Server Certificates and EFS 407
Chapter 11 Configuring & Managing Groups, Permissions, Rights, & Auditing 449
Appendix A Responding to Security Incidents 495
Glossary 511
Index 533
Contents

Introduction xxi

Assessment Test xxxiv

Chapter 1 Configuring, Deploying, and Troubleshooting Security Templates 1
  Group Policy Objects and Windows 2003 Server 3
    Configuring Group Policies 4
    Applying Group Policies 7
    Modifying Group Policy Inheritance 8
  Working with Security Templates 9
    Default Security Templates 12
    Incremental Templates 13
  Configuring Templates 14
    Account Policies 14
    .pol Files 16
    Audit Policies 16
    User Rights Assignment 21
    Security Options 22
    System Services 23
    Registry and File System Permissions 24
    Restricted Groups 26
    Event Logs 28
  Deploying Security Templates 29
    Using Group Policies to Deploy Templates 29
    Using Scripts to Deploy Templates 31
  Troubleshooting Security Templates 33
    Troubleshooting Group Policy–Applied Templates 34
    Troubleshooting after Upgrading Operating Systems 35
    Troubleshooting Mixed Client Environments 35
  Summary 35
  Exam Essentials 36
  Review Questions 37
  Answers to Review Questions 42

Chapter 2 Configuring Security Based on Computer Roles 45
  SQL Server Security 46
    Security Features in SQL Server 2000 47
    Windows Security and SQL Server 48
  Exchange Server Security 51
    Securing the SMTP Service 51
    Securing Outlook Web Access 52
Securing Outlook Web Access, URLScan, and IIS Lockdown 53
Securing Public Folder Information 53
Windows Domain Controller Security 53
Using Digital Signatures for Communication 54
Securing DNS Updates 55
Restricting Anonymous Access 55
Enabling NTLMv2 for Legacy Clients 57
Hardening the TCP/IP Stack 57
Disabling Auto Generation of 8.3 Filenames 58
Disabling LM Hash Creation 58
Securing Built-in Accounts 58
Infrastructure Security 59
DHCP 60
DNS 61
IIS 5 Server Security 62
IP Address/DNS Restrictions 66
Disabling the IIS Anonymous Account 67
The URLScan Tool 67
IIS 6 Server Security 70
Securing Mobile Communications and Internet Authentication Service (IAS) Server 71
Applying Security to Client Operating Systems 73
Unix Clients 73
NetWare Clients 74
Macintosh Clients 75
Summary 76
Exam Essentials 76
Review Questions 78
Answers to Review Questions 83

Chapter 3 Installing, Managing, & Troubleshooting Hotfixes & Service Packs 87
Determining the Current Status of Hotfixes and Service Packs 88
Installing Service Packs and Hotfixes 89
Using the MBSA Tool 92
Slipstreaming 101
Managing Service Packs and Hotfixes 105
Troubleshooting the Deployment of Service Packs and Hotfixes 119
Summary 121
Exam Essentials 122
Review Questions 123
Answers to Review Questions 128
The Next Steps 204
Implementing VPNs to Protect Wireless Networks 205
Combining VPN and 802.1x 206
Wireless Security Moving Forward 206
Summary 207
Exam Essentials 208
Review Questions 209
Answers to Review Questions 215

Chapter 6 Deploying, Managing, and Configuring SSL Certificates 217
An SSL Primer 219
Obtaining Public and Private Certificates 221
Obtaining Public Certificates 221
Obtaining and Renewing a Private Certificate 230
Configuring SSL to Secure Communications Channels 236
Using SSL to Secure a Client Machine to Web Server Traffic 236
Using SSL to Secure Web Server to SQL Server Traffic 239
Using SSL to Secure Client Machine to Active Directory Domain Controller Traffic 243
Using SSL to Secure Client Machine to E-Mail Server Traffic 246
Securing SMTP 249
Securing IMAP4 251
Securing POP3 254
Setting Up and Testing Secured IMAP4, POP3, and SMTP with Outlook Express 256
Securing Outlook Web Access 259
Summary 261
Exam Essentials 262
Review Questions 263
Answers to Review Questions 269

Chapter 7 Configuring, Managing, and Troubleshooting Authentication 271
Configuring and Troubleshooting Authentication 272
The LAN Authentication Protocols 273
The Logon Process 277
Troubleshooting Authentication 280
Configuring Authentication Protocols to Support Mixed Windows Client-Computer Environments 281
The Interoperability of Kerberos Authentication with Unix 284
Contents

Chapter 8 Configuring and Troubleshooting Virtual Private Network Protocols 321

VPNs and Internet Service Providers 322
Routing and Remote Access Services (RRAS) Server 324
Configuring RRAS 324
Configuring Authentication Protocols 327
Troubleshooting RRAS 327
Configuring and Troubleshooting VPN Client Systems 333
Configuring Client Systems for VPNs 333
Troubleshooting Client Systems 338
Network Address Translation (NAT) and VPNs 339
Firewall Servers with VPNs 340
Remote Access Policies 341
The Connection Manager Administration Kit 345
Summary 349
Exam Essentials 350
Review Questions 351
Answers to Review Questions 356

Chapter 9 Installing, Configuring, and Managing Certificate Authorities 357

Public Key Infrastructure and Certificate Authorities 358
Installing and Configuring the Root CA 361
Configuring the Publication of CRLs 364
Installing and Configuring the Intermediate CA 366
Installing and Configuring the Issuing CA 372
Contents

Configuring Certificate Templates 379
Configuring Public Key Group Policies 381
Prerequisites for Using Group Policies to Distribute Certificates 381
Configuring Certificate Enrollment and Renewals 386
Managing Certificate Authorities 390
Viewing Certificates 391
Revoking Certificates 392
Editing Certificates 393
Managing CRLs 394
Back Up and Restoring the CA 395
Summary 398
Exam Essentials 399
Review Questions 401
Answers to Review Questions 405

Chapter 10 Managing Client-Computer and Server Certificates and EFS 407

Managing Client Certificates 408
- Securing E-mail with Secure MIME 408
- Securing Files and Folders with the Encrypting File System (EFS) 415
- Importing and Exporting Certificates 418
- Certificate Storage 423
Publishing Certificates through Active Directory 425
- Publishing Certificates from a Stand-Alone Online CA 425
- Using Certificates in a Child Domain 427
Enrolling Certificates 430
- The Certificates MMC Snap-In 430
- Web Enrollment Pages 431
- Auto-Enrollment 433
Managing and Troubleshooting EFS 434
- Implementing EFS 434
- EFS Encryption for Domain Members 435
- EFS and Workgroup Members 436
- Disabling EFS 437
- Troubleshooting EFS 438
Summary 439
Exam Essentials 439
Review Questions 441
Answers to Review Questions 446
Chapter 11  Configuring & Managing Groups, Permissions, Rights, & Auditing

Windows Server 2003 Security Groups 450
Group Nesting 451
Understanding Windows Events 452
Event Messages in Event Viewer 452
Implementing and Configuring Auditing 457
Configuring Access Control Lists 470
User Rights 471
Using Event Logs 474
Managing Log Retention 480
Managing Distributed Audit Logs 481
Summary 486
Exam Essentials 486
Review Questions 488
Answers to Review Questions 493

Appendix A  Responding to Security Incidents

How to Recognize a Security Incident 496
Planning Your Response 498
Understanding the Types of Attacks 501
Natural Disasters 501
Hacker Attacks 501
Virus Attacks 502
Spyware 504
Denial of Service Attacks 504
Trojan Horse Attacks 505
Worm Attacks 505
Isolating and Containing the Incident 506
Preserving the Chain of Evidence 507
Implementing Countermeasures 508
Restoring Services 510
Summary 510

Index 533
## Table of Exercises

<table>
<thead>
<tr>
<th>Exercise</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Exercise  1.1</td>
<td>Configuring an Account Policy</td>
<td>16</td>
</tr>
<tr>
<td>Exercise  1.2</td>
<td>Configuring an Audit Policy</td>
<td>20</td>
</tr>
<tr>
<td>Exercise  1.3</td>
<td>Configuring a User Rights Policy</td>
<td>21</td>
</tr>
<tr>
<td>Exercise  1.4</td>
<td>Configuring the Last Logged-On Username So That It Doesn't</td>
<td>22</td>
</tr>
<tr>
<td></td>
<td>Appear in the Logon Dialog Box</td>
<td></td>
</tr>
<tr>
<td>Exercise  1.5</td>
<td>Configuring a System Service Security and Startup Policy</td>
<td>24</td>
</tr>
<tr>
<td>Exercise  1.6</td>
<td>Configuring a Registry Setting Policy</td>
<td>26</td>
</tr>
<tr>
<td>Exercise  1.7</td>
<td>Adding the Domain Administrators Global Security Group to a</td>
<td>28</td>
</tr>
<tr>
<td></td>
<td>New Security Group That You Have Created</td>
<td></td>
</tr>
<tr>
<td>Exercise  3.1</td>
<td>Installing a Service Pack for Windows 2000</td>
<td>92</td>
</tr>
<tr>
<td>Exercise  3.2</td>
<td>Installing the MBSA Tool</td>
<td>95</td>
</tr>
<tr>
<td>Exercise  3.3</td>
<td>Creating a Slipstreamed Installation Share Point</td>
<td>101</td>
</tr>
<tr>
<td>Exercise  3.4</td>
<td>Using QChain to Install a Series of Hotfixes</td>
<td>119</td>
</tr>
<tr>
<td>Exercise  4.1</td>
<td>Creating a Custom MMC for IPSec Management</td>
<td>137</td>
</tr>
<tr>
<td>Exercise  4.2</td>
<td>Setting IPSec to Run in Transport Mode</td>
<td>140</td>
</tr>
<tr>
<td>Exercise  4.3</td>
<td>Setting IPSec to Run in Tunnel Mode</td>
<td>141</td>
</tr>
<tr>
<td>Exercise  4.4</td>
<td>Creating a New MMC with the Certificate Snap-in</td>
<td>156</td>
</tr>
<tr>
<td>Exercise  5.1</td>
<td>Configuring a Public Wireless LAN with a Windows XP Professional Client.</td>
<td>177</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exercise  5.2</td>
<td>Configuring a Public Wireless LAN with a Windows 2000 Professional Client.</td>
<td>178</td>
</tr>
<tr>
<td>Exercise  5.3</td>
<td>Configuring a Private Wireless LAN with a Windows XP Professional Client.</td>
<td>180</td>
</tr>
<tr>
<td>Exercise  5.4</td>
<td>Configuring a Private Wireless LAN with a Windows 2000 Professional Client.</td>
<td>181</td>
</tr>
<tr>
<td>Exercise  5.5</td>
<td>Configuring WEP</td>
<td>192</td>
</tr>
<tr>
<td>Exercise  6.1</td>
<td>Obtaining a Public Certificate</td>
<td>224</td>
</tr>
<tr>
<td>Exercise  6.2</td>
<td>Installing an SSL Certificate</td>
<td>227</td>
</tr>
<tr>
<td>Exercise  6.3</td>
<td>Renewing a Certificate</td>
<td>228</td>
</tr>
<tr>
<td>Exercise  6.4</td>
<td>Obtaining a Private Certificate Using the Web Interface</td>
<td>231</td>
</tr>
<tr>
<td>Exercise  6.5</td>
<td>Obtaining a Private Certificate Using an Online CA</td>
<td>234</td>
</tr>
<tr>
<td>Exercise  6.6</td>
<td>Installing the Certificates Snap-In</td>
<td>235</td>
</tr>
<tr>
<td>Exercise  6.7</td>
<td>Renewing a Private Certificate</td>
<td>235</td>
</tr>
<tr>
<td>Exercise  6.8</td>
<td>Enforcing SSL on IIS 6</td>
<td>238</td>
</tr>
<tr>
<td>Exercise</td>
<td>Description</td>
<td>Page</td>
</tr>
<tr>
<td>----------</td>
<td>------------------------------------------------------------------------------</td>
<td>------</td>
</tr>
<tr>
<td>6.9</td>
<td>Installing a Certificate on a SQL Server</td>
<td>240</td>
</tr>
<tr>
<td>6.10</td>
<td>Adding a CA to the Trusted Root Certification Authorities List</td>
<td>241</td>
</tr>
<tr>
<td>6.11</td>
<td>Configuring GPO for Automated Certificate Distribution for Domain Controllers</td>
<td>244</td>
</tr>
<tr>
<td>6.12</td>
<td>Testing SSL-Secured LDAP to Active Directory</td>
<td>245</td>
</tr>
<tr>
<td>6.13</td>
<td>Creating a Dedicated SMTP Virtual Server</td>
<td>249</td>
</tr>
<tr>
<td>6.15</td>
<td>Securing IMAP4 on Exchange</td>
<td>252</td>
</tr>
<tr>
<td>6.16</td>
<td>Securing POP3 on Exchange 2000 Server</td>
<td>254</td>
</tr>
<tr>
<td>6.17</td>
<td>Testing Secure E-Mail with Outlook Express</td>
<td>256</td>
</tr>
<tr>
<td>6.18</td>
<td>Securing OWA</td>
<td>260</td>
</tr>
<tr>
<td>7.1</td>
<td>Disabling LM and NTLM version 1</td>
<td>274</td>
</tr>
<tr>
<td>7.2</td>
<td>Installing the Directory Services Client</td>
<td>282</td>
</tr>
<tr>
<td>7.3</td>
<td>Disabling LM and NTLM Version 1 Authentication in Windows NT 4</td>
<td>284</td>
</tr>
<tr>
<td>7.4</td>
<td>Configuring Windows XP Professional to Use a Third-Party Kerberos Version 5 Implementation</td>
<td>285</td>
</tr>
<tr>
<td>7.5</td>
<td>Creating a One-Way Trust: A Windows NT 4 Domain Trusts an Active Directory Domain</td>
<td>290</td>
</tr>
<tr>
<td>7.6</td>
<td>Configuring Anonymous Authentication in IIS 6</td>
<td>293</td>
</tr>
<tr>
<td>7.7</td>
<td>Enabling Basic Authentication in IIS 6</td>
<td>294</td>
</tr>
<tr>
<td>7.8</td>
<td>Enabling Digest Authentication in IIS 6</td>
<td>296</td>
</tr>
<tr>
<td>7.9</td>
<td>Enabling Integrated Windows Authentication in IIS 6</td>
<td>299</td>
</tr>
<tr>
<td>7.10</td>
<td>Implementing Passport Authentication</td>
<td>301</td>
</tr>
<tr>
<td>7.11</td>
<td>Configuring Certificate Mapping</td>
<td>303</td>
</tr>
<tr>
<td>7.12</td>
<td>Configuring RRAS Authentication Protocols</td>
<td>307</td>
</tr>
<tr>
<td>7.13</td>
<td>Enabling EAP on RRAS</td>
<td>309</td>
</tr>
<tr>
<td>8.1</td>
<td>Configuring RRAS for VPN</td>
<td>325</td>
</tr>
<tr>
<td>8.2</td>
<td>Creating and Deleting VPN Ports</td>
<td>326</td>
</tr>
<tr>
<td>8.3</td>
<td>Manually Configuring PPTP Filtering</td>
<td>330</td>
</tr>
<tr>
<td>8.4</td>
<td>Configuring a Windows XP Professional VPN Client</td>
<td>334</td>
</tr>
<tr>
<td>8.5</td>
<td>Configuring a Windows 2000 Professional VPN client</td>
<td>335</td>
</tr>
<tr>
<td>8.6</td>
<td>Running the Connection Manager Administration Kit</td>
<td>346</td>
</tr>
<tr>
<td>9.1</td>
<td>Installing a Stand-Alone Root CA</td>
<td>362</td>
</tr>
<tr>
<td>9.2</td>
<td>Creating the CDP for the Stand-Alone Offline Root CA</td>
<td>364</td>
</tr>
<tr>
<td>9.3</td>
<td>Installing an Intermediate CA</td>
<td>367</td>
</tr>
<tr>
<td>9.4</td>
<td>Installing an Issuing Enterprise CA</td>
<td>373</td>
</tr>
</tbody>
</table>
### Table of Exercises

<table>
<thead>
<tr>
<th>Exercise</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>9.5</td>
<td>Viewing Published Certificates and CRLs in Active Directory</td>
<td>378</td>
</tr>
<tr>
<td>9.6</td>
<td>Adding and Deleting Certificate Templates.</td>
<td>380</td>
</tr>
<tr>
<td>9.7</td>
<td>Configuring the Automatic Certificate Request Group Policy</td>
<td>381</td>
</tr>
<tr>
<td>9.8</td>
<td>Configuring the Trusted Root Certification Authorities List Using Group Policy</td>
<td>383</td>
</tr>
<tr>
<td>9.9</td>
<td>Configuring the Enterprise Trust List Using Group Policy</td>
<td>384</td>
</tr>
<tr>
<td>9.10</td>
<td>Using the Web Enrollment Pages to Manually Request a Certificate</td>
<td>387</td>
</tr>
<tr>
<td>9.11</td>
<td>Using the Certificates MMC Snap-In to Enroll for User and Computer Certificates and for Renewing Certificates</td>
<td>388</td>
</tr>
<tr>
<td>9.12</td>
<td>Revoking a Certificate</td>
<td>393</td>
</tr>
<tr>
<td>9.13</td>
<td>Backing Up the CA</td>
<td>396</td>
</tr>
<tr>
<td>9.14</td>
<td>Restoring the CA</td>
<td>397</td>
</tr>
<tr>
<td>10.1</td>
<td>Using S/MIME to Sign and Seal E-mail</td>
<td>410</td>
</tr>
<tr>
<td>10.2</td>
<td>Using EFS to Encrypt Files</td>
<td>417</td>
</tr>
<tr>
<td>10.3</td>
<td>Exporting a Certificate</td>
<td>420</td>
</tr>
<tr>
<td>10.4</td>
<td>Importing a Certificate</td>
<td>422</td>
</tr>
<tr>
<td>10.5</td>
<td>Configuring and Publishing a Certificate from a Stand-Alone CA</td>
<td>425</td>
</tr>
<tr>
<td>10.6</td>
<td>Enabling Child Domain Users to Enroll Certificates and Configure Publication to Active Directory</td>
<td>427</td>
</tr>
<tr>
<td>10.7</td>
<td>Using the Certificates MMC Snap-In</td>
<td>430</td>
</tr>
<tr>
<td>10.8</td>
<td>Using Web Enrollment</td>
<td>432</td>
</tr>
<tr>
<td>10.9</td>
<td>Configuring Group Policies to Support Auto-Enrollment</td>
<td>433</td>
</tr>
<tr>
<td>10.10</td>
<td>Configuring the Shortcut Menu</td>
<td>434</td>
</tr>
<tr>
<td>11.1</td>
<td>Enabling Auditing Using a Group Policy</td>
<td>458</td>
</tr>
<tr>
<td>11.2</td>
<td>Changing the Logging Option for a Website to Log Its Events to a SQL Database</td>
<td>475</td>
</tr>
<tr>
<td>11.3</td>
<td>Running a Packet Trace on Your Windows Server 2003 Server Machine</td>
<td>478</td>
</tr>
<tr>
<td>11.4</td>
<td>Configuring RAS Logging on Your Windows Server 2003 Server Machine</td>
<td>479</td>
</tr>
<tr>
<td>11.5</td>
<td>Searching for Domain Controller Restarts Using the EventComb Utility</td>
<td>485</td>
</tr>
</tbody>
</table>