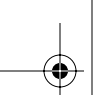
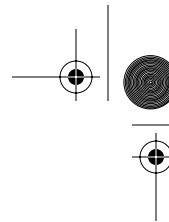


Contents at a Glance

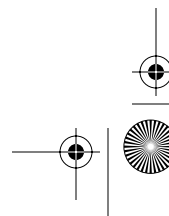
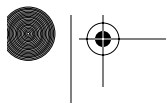
<i>Introduction</i>	<i>xxi</i>
<i>Assessment Test</i>	<i>xxxiv</i>
Chapter 1 Configuring, Deploying, and Troubleshooting Security Templates	1
Chapter 2 Configuring Security Based on Computer Roles	45
Chapter 3 Installing, Managing, & Troubleshooting Hotfixes & Service Packs	87
Chapter 4 Configuring IPSec 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
<i>Index</i>	<i>533</i>





Contents

<i>Introduction</i>		<i>xxi</i>
<i>Assessment Test</i>		<i>xxxiv</i>
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



xii Contents

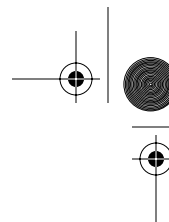
Securing Outlook Web Access, URLScan, and IIS Lockdown	53
Securing Public Folder Information	53
Windows Domain Controller Security	53
Using Digital Signatures for Communication	54
Securing DNS Updates	55
Restricting Anonymous Access	55
Enabling NTLMv2 for Legacy Clients	57
Hardening the TCP/IP Stack	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

Chapter 4	Configuring IPSec and SMB Signing	131
	Understanding IPSec	133
	Configuring and Administering IPSec Authentication	136
	Configuring the Appropriate IPSec Protocol and Encryption Levels	149
	Deploying and Managing IPSec Certificates	151
	Renewing Certificates	153
	Securing Communication between Server Types with IPSec	153
	Troubleshooting IPSec	154
	Domain Controllers and SMB Signing	158
	SMB Commands	159
	Configuring SMB	160
	The Common Internet File System (CIFS)	160
	Enabling SMB Signing	160
	Network Analyzers	164
	Summary	165
	Exam Essentials	166
	Review Questions	167
	Answers to Review Questions	172
Chapter 5	Implementing Security for Wireless Networks	175
	Configuring Public and Private Wireless LANs	176
	Configuring a Public Wireless LAN	177
	Configuring a Private Wireless LAN	179
	Configuring Windows CE as a Wireless Client	182
	Wireless Components	182
	Configuring Secure Wireless Network Settings	185
	Dynamic Host Configuration Protocol (DHCP)	185
	Service Set Identifier (SSID)	186
	SSID Security Concerns	189
	Configuring Wireless Encryption Levels with WEP	190
	Wi-Fi Protected Access (WPA)	194
	MAC Filtering	195
	Configuring Wireless Encryption Levels Using 802.1x	197
	EAP Authentication Methods	200
	Problems and Attacks Specific to Wireless Networks	201
	Rogue APs	201
	War Driving	202
	War Chalking	202
	Radio Interference	203
	WEP Attacks	203

xiv Contents

	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

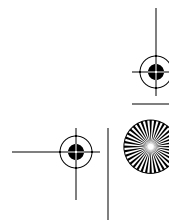
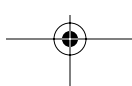
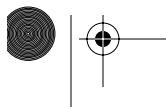
	Configuring Authentication in Extranet Scenarios and with Members of Nontrusted Domains	286
	Trust Relationships	288
	Configuring and Troubleshooting Authentication for Web Users	291
	Anonymous Authentication	292
	Configuring and Troubleshooting Authentication for Secure Remote Access	306
	Multifactor Authentication with Smart Cards and EAP	310
	Summary	311
	Exam Essentials	311
	Review Questions	313
	Answers to Review Questions	318
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
	Managing Client Computer Configurations for Remote Access Security	341
	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



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
Backing 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	449
	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	495
	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
<i>Index</i>		533

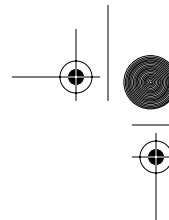


Table of Exercises

Exercise 1.1	Configuring an Account Policy	16
Exercise 1.2	Configuring an Audit Policy	20
Exercise 1.3	Configuring a User Rights Policy	21
Exercise 1.4	Configuring the Last Logged-On Username So That It Doesn't Appear in the Logon Dialog Box	22
Exercise 1.5	Configuring a System Service Security and Startup Policy	24
Exercise 1.6	Configuring a Registry Setting Policy	26
Exercise 1.7	Adding the Domain Administrators Global Security Group to a New Security Group That You Have Created	28
Exercise 3.1	Installing a Service Pack for Windows 2000	92
Exercise 3.2	Installing the MBSA Tool	95
Exercise 3.3	Creating a Slipstreamed Installation Share Point	101
Exercise 3.4	Using QChain to Install a Series of Hotfixes	119
Exercise 4.1	Creating a Custom MMC for IPsec Management	137
Exercise 4.2	Setting IPsec to Run in Transport Mode	140
Exercise 4.3	Setting IPsec to Run in Tunnel Mode	141
Exercise 4.4	Creating a New MMC with the Certificate Snap-in.	156
Exercise 5.1	Configuring a Public Wireless LAN with a Windows XP Professional Client.	177
Exercise 5.2	Configuring a Public Wireless LAN with a Windows 2000 Professional Client.	178
Exercise 5.3	Configuring a Private Wireless LAN with a Windows XP Professional Client.	180
Exercise 5.4	Configuring a Private Wireless LAN with a Windows 2000 Professional Client.	181
Exercise 5.5	Configuring WEP	192
Exercise 6.1	Obtaining a Public Certificate	224
Exercise 6.2	Installing an SSL Certificate	227
Exercise 6.3	Renewing a Certificate	228
Exercise 6.4	Obtaining a Private Certificate Using the Web Interface	231
Exercise 6.5	Obtaining a Private Certificate Using an Online CA	234
Exercise 6.6	Installing the Certificates Snap-In	235
Exercise 6.7	Renewing a Private Certificate	235
Exercise 6.8	Enforcing SSL on IIS 6	238

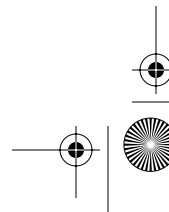
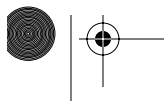


Table of Exercises **xix**

Exercise 6.9	Installing a Certificate on a SQL Server240
Exercise 6.10	Adding a CA to the Trusted Root Certification Authorities List241
Exercise 6.11	Configuring GPO for Automated Certificate Distribution for Domain Controllers244
Exercise 6.12	Testing SSL-Secured LDAP to Active Directory245
Exercise 6.13	Creating a Dedicated SMTP Virtual Server249
Exercise 6.14	Securing SMTP on Exchange 2000 Server250
Exercise 6.15	Securing IMAP4 on Exchange252
Exercise 6.16	Securing POP3 on Exchange 2000 Server254
Exercise 6.17	Testing Secure E-Mail with Outlook Express256
Exercise 6.18	Securing OWA260
Exercise 7.1	Disabling LM and NTLM version 1274
Exercise 7.2	Installing the Directory Services Client282
Exercise 7.3	Disabling LM and NTLM Version 1 Authentication in Windows NT 4284
Exercise 7.4	Configuring Windows XP Professional to Use a Third-Party Kerberos Version 5 Implementation285
Exercise 7.5	Creating a One-Way Trust: A Windows NT 4 Domain Trusts an Active Directory Domain290
Exercise 7.6	Configuring Anonymous Authentication in IIS 6293
Exercise 7.7	Enabling Basic Authentication in IIS 6294
Exercise 7.8	Enabling Digest Authentication in IIS 6296
Exercise 7.9	Enabling Integrated Windows Authentication in IIS 6299
Exercise 7.10	Implementing Passport Authentication301
Exercise 7.11	Configuring Certificate Mapping303
Exercise 7.12	Configuring RRAS Authentication Protocols307
Exercise 7.13	Enabling EAP on RRAS309
Exercise 8.1	Configuring RRAS for VPN325
Exercise 8.2	Creating and Deleting VPN Ports326
Exercise 8.3	Manually Configuring PPTP Filtering330
Exercise 8.4	Configuring a Windows XP Professional VPN Client334
Exercise 8.5	Configuring a Windows 2000 Professional VPN client335
Exercise 8.6	Running the Connection Manager Administration Kit346
Exercise 9.1	Installing a Stand-Alone Root CA362
Exercise 9.2	Creating the CDP for the Stand-Alone Offline Root CA364
Exercise 9.3	Installing an Intermediate CA367
Exercise 9.4	Installing an Issuing Enterprise CA373

xx Table of Exercises

Exercise 9.5	Viewing Published Certificates and CRLs in Active Directory	378
Exercise 9.6	Adding and Deleting Certificate Templates.	380
Exercise 9.7	Configuring the Automatic Certificate Request Group Policy	381
Exercise 9.8	Configuring the Trusted Root Certification Authorities List Using Group Policy	383
Exercise 9.9	Configuring the Enterprise Trust List Using Group Policy.	384
Exercise 9.10	Using the Web Enrollment Pages to Manually Request a Certificate . . .	387
Exercise 9.11	Using the Certificates MMC Snap-In to Enroll for User and Computer Certificates and for Renewing Certificates	388
Exercise 9.12	Revoking a Certificate	393
Exercise 9.13	Backing Up the CA.	396
Exercise 9.14	Restoring the CA	397
Exercise 10.1	Using S/MIME to Sign and Seal E-mail	410
Exercise 10.2	Using EFS to Encrypt Files	417
Exercise 10.3	Exporting a Certificate	420
Exercise 10.4	Importing a Certificate	422
Exercise 10.5	Configuring and Publishing a Certificate from a Stand-Alone CA	425
Exercise 10.6	Enabling Child Domain Users to Enroll Certificates and Configure Publication to Active Directory.	427
Exercise 10.7	Using the Certificates MMC Snap-In	430
Exercise 10.8	Using Web Enrollment	432
Exercise 10.9	Configuring Group Policies to Support Auto-Enrollment	433
Exercise 10.10	Configuring the Shortcut Menu	434
Exercise 10.11	Configuring a Recovery Policy on a Stand-alone Windows Server 2003 Computer	436
Exercise 11.1	Enabling Auditing Using a Group Policy.	458
Exercise 11.2	Changing the Logging Option for a Website to Log Its Events to a SQL Database.	475
Exercise 11.3	Running a Packet Trace on Your Windows Server 2003 Server Machine	478
Exercise 11.4	Configuring RAS Logging on Your Windows Server 2003 Server Machine	479
Exercise 11.5	Searching for Domain Controller Restarts Using the EventComb Utility	485