



Contents

Foreword	xxxiii
❖ Part I Implementing, Managing, and Troubleshooting	
Baseline Security	1
Chapter 1 Basic Windows 2000 Security: Using Security	
Templates	3
Introduction	4
Windows 2000 Active Directory Review	4
Introduction to Directory Services	5
History of the Windows Directory Service	6
Active Directory Architecture	9
The X.500 Directory Standard	11
The Logical Structure of Active Directory	12
Forests	12
Trees	13
Domains	13
Schema	13
Global Catalog	14
Organizational Units	14
Groups	15
The Physical Structure of Active Directory	17
Sites	17
Domain Controllers	17
Servers and Workstations	18
Objects: The Heart of It All	18
Containers: Odd Men Out	19
The Basic Windows 2000 Security Tools	20
Security Configuration Tool Set	20
Security Templates	21
Group Policy Security Settings	23
Security Configuration and Analysis	27
The Command-Line Tools	30
Secedit.exe	30
Gpresult.exe and Gpotool.exe	31
Creating the Security Configuration Tool Set User Interface	31
1.1 Configuring Basic Windows 2000 Security with Templates	32

1.1.2	Account Policies	33
1.1.3/	Local Policies	35
1.1.4/		
1.1.5		
1.1.8	Event Log	42
1.1.7	Restricted Groups	44
1.1.6	System Services	46
1.1.1	Registry	48
1.1.1	File System	50
1.2	Deploying Security Templates	53
	Let's Configure!	54
	Deploying Security via Group Policy	57
	Deploying Security via Scripting	60
1.2	Analyzing Your Security Configuration	63
	Using Security Configuration and Analysis	63
	Examining the Analysis Results	65
	Using Secedit.exe	67
	<i>secedit /analyze</i>	67
	<i>secedit /refreshpolicy</i>	68
	<i>secedit /export</i>	68
	<i>secedit /validate</i>	69
	Areas	69
	Analyzing Security with Secedit.exe	70
	Using Gpresult.exe and Gpoutil.exe	71
	Summary of Exam Objectives	73
	Exam Objectives Fast Track	74
	Exam Objectives Frequently Asked Questions	76
	Self Test	77
	Self Test Quick Answer Key	84
	Chapter 2 Advanced Security Template and Group Policy Issues	85
	Introduction	86
1.4	Configuring Role-Based Server Security	86
	Securing the Domain	88
	Windows 2000 Domain Controllers	89
	Member Servers	92
	SQL Server 2000.....	93
	Exchange 2000 Server.....	97

	Windows 2000 Internet Information Services Servers	99
	Windows 2000 Internet Access Service Servers	106
1.5	Creating Secure Workstations	107
	Desktop Workstations	107
	Portable Computers	111
1.3	Security Template Application Issues	112
	Upgrade Installations	112
	Legacy Client Issues	113
	Using Gpresult.exe	114
	Event Log Entries	114
	Last Thoughts on Security Templates	117
3.4	Securing Server Message Block Traffic	118
	Summary of Exam Objectives	120
	Exam Objectives Fast Track	121
	Exam Objectives Frequently Asked Questions	122
	Self Test	124
	Self Test Quick Answer Key	130
❖	Part II Implementing, Managing, and Troubleshooting	
	Service Packs and Security Updates	131
	Chapter 3 Identifying, Installing, and Troubleshooting	
	Required Updates	133
	Introduction	134
2.1	Identifying Required Updates	134
	Types of Updates	134
	Service Packs	134
	Hotfixes	135
	Analyzing Your Computers	137
	Visiting Windows Update	137
	The Microsoft Network Security Hotfix Checker	139
	The Microsoft Baseline Security Analyzer	145
2.2/2.3	Deploying and Managing Updates	152
2.2.1	Installing Updates on New Computers	155
	Slipstreaming Installation Media for RIS Deployment	155
	Scripting Updates	163
	Installing Updates in Isolated Networks	165
	Deployment Updates to Existing Computers	165
	Windows Update	165
	Windows Update Catalog	169

- Software Update Service and Automatic Updates172
 - Systems Management Server.....180
 - Special Considerations for Updating Servers181
- 2.4** Troubleshooting Update Installations182
 - Application Compatibility Issues182
 - Permissions Problems182
 - Version Conflicts183
- Summary of Exam Objectives184
- Exam Objectives Fast Track186
- Exam Objectives Frequently Asked Questions187
- Self Test189
- Self Test Quick Answer Key196
- ❖ Part III Implementing and Managing a Public Key Infrastructure (PKI) and Encrypting File System (EFS)197**
 - Chapter 4 Installing, Configuring, & Managing Windows 2000 Certificate Authorities.....199**
 - Introduction200
 - Cryptography and You: What is it All About?200
 - Public Key Cryptography201
 - Public Key Functionality203
 - Digital Signatures203
 - Authentication204
 - Secret Key Agreement via Public Key206
 - Bulk Data Encryption without Prior Shared Secrets206
 - Protecting and Trusting Cryptographic Keys206
 - Certificates207
 - 3.1.4** Certificate Authorities208
 - CA Types209
 - Certificate Hierarchies211
 - Trust and Validation212
 - 5.1/** Installing and Managing Windows 2000 Certificate Authorities212
 - 5.1.1/**
 - 5.2**
 - 3.5.1/** Requesting a Certificate.....217
 - 3.5.3/**
 - 5.1.5/**
 - 5.1.6/**
 - 5.2.1**

3.5.1/	Exporting and Importing Certificates	222
3.5.3/		
5.1.6		
5.2.2	Revoking Certificates.....	226
5.1.3/	Configuring Publication of CRLs	229
5.2.3		
5.1.2	Configuring Certificate Templates	231
5.1.4	Configuring Public Key Group Policy	234
	Configuring Automatic Certificate Enrollment	234
	Configuring the Trusted Root CAs	236
5.2.4	Backing Up and Restoring Certificate Services	237
5.3	Advanced Certificate Management Issues	240
5.3.1	Publishing Certificates in Active Directory	241
5.3.3	Recovering Key Management Server Issued Keys	241
5.3.2	Windows XP Auto-enrollment	244
	Summary of Exam Objectives	247
	Exam Objectives Fast Track	249
	Exam Objectives Frequently Asked Questions	253
	Self Test	255
	Self Test Quick Answer Key	261
	Chapter 5 Managing and Troubleshooting the	
	Encrypting File System	263
	Introduction	264
	The Role of EFS in a Network Security Plan.....	265
	Using the Encrypting File System	266
	Encryption Fundamentals	267
	Public Key, or Asymmetric Cryptography	268
	Secret Key, or Symmetric Cryptography	269
	How EFS Works	269
5.4	User Operations	271
	Encrypting a File or Folder	272
	Encrypting a File or Folder on the Local Computer	272
	Encrypting a File or Folder on a Remote Computer	274
	Accessing an Encrypted File	275
	Copying an Encrypted File	276
	Preventing Files from Being Encrypted on a Server	277
	Moving or Renaming an Encrypted File	278
	Sharing an Encrypted File in Windows XP/.NET	278

- Decrypting a File279
- Using the Cipher Utility in Windows 2000280
- Encrypting a Directory282
- Employing Recovery Operations283
- 5.4 EFS Architecture and Troubleshooting292**
 - EFS Components292
 - The Encryption Process295
 - The EFS File Information298
 - The Decryption Process300
 - Troubleshooting EFS302
 - Summary of Exam Objectives304
 - Exam Objectives Fast Track305
 - Exam Objectives Frequently Asked Questions307
 - Self Test310
 - Self Test Quick Answer Key316
- ❖ Part IV: Implementing, Managing, and Troubleshooting**
- Secure Communication Channels317**
- Chapter 6 Configuring and Troubleshooting**
- Windows IP Security319**
 - Introduction320
 - The Need for Network Security321
 - Snooping321
 - Spoofing322
 - The TCP/IP Sequence Number Attack322
 - Spoofing Tools322
 - Password Compromise323
 - DoS Attacks325
 - TCP SYN Attacks325
 - SMURF Attacks325
 - Teardrop Attacks326
 - Ping-of-Death Attacks326
 - MITM Attacks326
 - Application-directed Attacks327
 - Compromised Key Attacks327
 - IP Security Overview328
 - Overview of IPSec Cryptographic Services329
 - Message Integrity329
 - Message Authentication331

3.1.2	Confidentiality	334
3.1.3	IPSec Security Services	335
	The AH	335
	ESP	336
	Security Associations and IPSec Key Management	
	Procedures	337
	Security Associations	337
	IPSec Key Management	337
	IP Security Management Tools	339
	IP Security Policies on Local Machine	339
	IP Security Monitor	340
	IPSec Policy Agent Service	342
	TCP/IP Advanced Options	343
	Certificates Snap-In	343
	Security Log	344
	NetDiag	344
3.1/	Deploying and Troubleshooting Windows IP Security	345
3.1.1/		
3.2	Evaluating Information	345
	Evaluating the “Enemy”	346
	Determining Required Security Levels	347
	Building Security Policies with Customized	
	IPSec Consoles	347
	Flexible Security Policies	349
	Rules	352
	Flexible Negotiation Policies	355
	Filters	356
	Creating a Security Policy	358
	Making the Rule	359
	Compatibility Notes	369
	Troubleshooting IP Security	369
	Summary of Exam Objectives	372
	Exam Objectives Fast Track	373
	Exam Objectives Frequently Asked Questions	375
	Self Test	376
	Self Test Quick Answer Key	381

	Chapter 7 Implementing Secure Wireless Networks	383
	Introduction to the Wireless LAN	384
	Benefits of the Wireless LAN	384
	Convenience	384
	Productivity	388
	Wireless LAN Concepts	388
	Communication in a Wireless Network	389
	Wireless Network Architecture	392
	IEEE 802.11 Wireless Local Area Networks	394
	IEEE 802.11b	395
	IEEE 802.11a	396
	IEEE 802.11g	396
	802.11 Communication Modes	397
3.3.2	Wired Equivalent Privacy	398
	Creating Privacy with WEP	400
	Authentication	401
3.3.2	802.1x Authentication	403
	User Identification and Strong Authentication	405
	Dynamic Key Derivation	405
	Mutual Authentication	406
	Per-Packet Authentication	406
3.3	Wireless LAN Security Issues	407
	Passive Attacks on Wireless Networks	407
	War Driving	408
	Sniffing	412
	Active Attacks on Wireless Networks	413
	Spoofing and Unauthorized Access	414
	Denial of Service and Flooding Attacks	416
	Man-in-the-Middle Attacks on Wireless Networks	418
	Network Hijacking and Modification	419
	Jamming Attacks	420
3.3	Wireless LAN Security: It's Not Perfect	421
	WEP Vulnerabilities	422
	Vulnerability to Plaintext Attacks	422
	Vulnerability of RC4 Algorithm	423
	Stream Cipher Vulnerability	423
3.3	Should You Use WEP?	425
	Security of 64-Bit Versus 128-Bit Keys	425

3.3	IEEE 802.1x Vulnerabilities	426
3.3.1/	Configuring Windows Client Computers for	
3.3.3	Wireless LAN Security	427
	Windows XP Professional	427
	Windows 2000 Professional	429
3.3	Additional Security Measures for Wireless LANs	431
	Using a Separate Subnet for Wireless Networks	431
	Using VPNs for Wireless Access to Wired Networks	432
	Temporal Key Integrity Protocol	434
	Message Integrity Code	434
	The IEEE 802.11i Standard	435
3.3	Implementing Wireless LAN Security:	
	Common Best Practices	436
	Summary of Exam Objectives	439
	Exam Objectives Fast Track	441
	Exam Objectives Frequently Asked Questions	445
	Self Test	446
	Self Test Quick Answer Key	451
❖	Part V Configuring, Managing, and Troubleshooting	
	Authentication and Remote Access Security	453
	Chapter 8 Configuring Secure Network and Internet	
	Authentication Methods	455
	Introduction	456
	Network Authentication in Windows 2000	456
	NTLM	457
	Kerberos	458
	Kerberos Overview	459
	Kerberos Concepts	460
	The Authenticator	461
	The KDC	462
	The Session Ticket (ST)	464
	The TGT	466
	Kerberos Authentication across Domain Boundaries	467
	Delegation of Authentication	468
	Proxy Tickets	469
	Forwarded Tickets	469
	Kerberos in Windows 2000	470
	The KDC and Account Database	471

	Kerberos Policy	473
	Delegation of Authentication	474
	Preauthentication	477
	Credentials Cache	478
	DNS Name Resolution	478
	Authorization Data.....	479
	KDC and Authorization Data	479
	Services and Authorization Data	480
	UDP and TCP Ports	480
4.1.4	Configuring Kerberos Trusts.....	480
	The Great Link: Kerberos Trusts between Domains	482
	Taking a Shortcut	483
4.1/	Configuring User Authentication.....	488
4.1.1		
4.1.3	Authentication for External Users	488
4.1.2	Configuring Interoperability with UNIX Servers	489
	Using Cleartext Authentication	489
	Using Certificate-based Authentication	489
	Using the Kerberos v5 Protocol	490
	Using NTLM Authentication	490
	Configuring Interoperability with Legacy Windows Clients	490
	Defining LM and NLM Authentication	491
	Using the Directory Services Client.....	491
	Deploying NTLM Version 2	492
	Making Clients Use NTLMv2	494
4.1.5/	Configuring Web Authentication	497
4.2		
	Using Anonymous Authentication	497
	Using Basic Authentication	497
	Using Digest Authentication	498
	Using Integrated Windows Authentication	500
	Using Client Certificate Mapping	500
	One-to-One Certificate Mapping	501
	Many-to-One Certificate Mapping	501
	Combining Authentication Methods	502
3.5/3.5.2/	Configuring Web Site Authentication	502
3.6		
	Troubleshooting Web Authentication.....	510

Summary of Exam Objectives	512
Exam Objectives Fast Track	513
Exam Objectives Frequently Asked Questions	517
Self Test	519
Self Test Quick Answer Key	525
Chapter 9 Configuring and Troubleshooting	
Remote Access and VPN Authentication.....	527
Introduction	528
4.3 Remote Access Authentication Methods	529
Point-to-Point Protocol	529
Password Authentication Protocol	530
Challenge Handshake Authentication Protocol	530
Microsoft Challenge Handshake Authentication Protocol	530
MS-CHAP v2	531
Extensible Authentication Protocol	532
EAP-MD5 CHAP	532
EAP-TLS	532
EAP and Smartcards/Certificates	533
4.4 Configuring a Remote Access Server	534
Installing and Configuring the Remote Access Server	535
Working with RAS Ports	541
4.4 Configuring a Virtual Private Networking Server	546
Installing and Configuring the VPN Server	547
Working with VPN Ports	556
Point-to-Point Tunneling Protocol	556
Layer 2 Tunneling Protocol	557
Internet Protocol Security	558
Configuring L2TP Ports	561
Configuring Remote Access Policies	562
Configuring Remote Access Profiles	567
Dial-in Constraints	567
IP	568
Multilink	569
Authentication	570
Encryption	570
Advanced	571
Remote Access Policy Administrative Models	571
4.3/4.4 Configuring Network Clients for Secure Remote Access	573

- 4.5 Using the Connection Manager Administration Kit576
 - Manually Creating the Connections577
 - Creating a Static Phone Book578
 - Creating a Dynamic Phone Book.....579
 - Running the CMAK580
 - Allowing Users to Use the Connection Manager582
- Troubleshooting Remote Access Problems582
 - Problems with a VPN Due to the Internet
 - Service Provider584
 - Client Computer Operating System Issues585
 - Network Address Translation Devices586
 - Routing and Remote Access Server Issues588
 - Firewall Issues589
- Summary of Exam Objectives591
- Exam Objectives Fast Track594
- Exam Objectives Frequently Asked Questions596
- Self Test598
- Self Test Quick Answer Key604
- ❖ **Part VI Monitoring and Responding to Security Incidents605**
 - Chapter 10 Configuring and Using Auditing and the Event Logs607**
 - Introduction608
 - Auditing for Increased Security609
 - 6.1 Auditing Windows 2000611
 - Windows 2000 Local Auditing611
 - Audit Account Logon Events611
 - Audit Account Management.....612
 - Audit Logon Events613
 - Audit Object Events613
 - Audit Policy Change.....613
 - Audit Privilege Use614
 - Audit Process Tracking615
 - Audit System Events616
 - Auditing with Group Policy620
 - Events to Audit621
 - Logon Events that Appear in the Event Log.....622

6.1/	Auditing Best Practices	627
6.1.1/		
6.2	Security Analysis	628
	Event Viewer Log Size	629
6.1	Auditing Internet Information Services	630
	Internet Information Services	630
6.1.2	Windows Auditing Tools	633
	The Dump Event Log	634
	EventCombMT	635
	Summary of Exam Objectives	638
	Exam Objectives Fast Track	639
	Exam Objectives Frequently Asked Questions	641
	Self Test	642
	Self Test Quick Answer Key	648
	Chapter 11 Responding to and Recovering from Security Breaches	649
	Introduction	650
6.3	Security Incidents	650
	Minimizing Security Incidents	651
	Hackers	655
	Hacker Jargon	655
6.3	Malware Issues	657
	Viruses	658
	Worms	659
	Trojan Horses	659
	Trojan Awareness	663
	Denial of Service	666
	Launching a Distributed DoS	669
6.3/	Incident Response	672
6.3.2/		
6.3.3	Defining an Incident Response Plan	672
	Forensics	673
	Conceptual Knowledge	674
	Your Role	675
6.3.1	Chain of Custody	678

- Evidence Collection679
- Summary of Exam Objectives681
- Exam Objectives Fast Track682
- Exam Objectives Frequently Asked Questions683
- Self Test685
- Self Test Quick Answer Key692
- ❖ **Part VII Appendices693**
 - Appendix A Utilities for the White Hat695**
 - Introduction696
 - White Hat Vulnerability Testing698
 - LANguard Network Scanner698
 - Network Mapper and Network Mapper for Windows701
 - Ethereal703
 - White Hat Protection Tools705
 - SSH705
 - PGP706
 - Summary707
 - Appendix B Port Numbers and Associated Attacks709**
 - Introduction710
 - Port Numbers710
 - Appendix C Self Test Questions, Answers, and Explanations717**
 - Index811**