Contents

Answers to Your Frequently Asked Questions

Q: How can I enable my Windows 98 clients to use Kerberos v5 authentication?

A: Down-level clients (Windows 9x and NT 4.0) do not support Kerberos v5 authentication. The only way to use Kerberos would be to upgrade your Windows 98 clients to Windows 2000 Professional.

Chapter 1 The Windows 2000 Server Security Migration Path 1

Introduction 2

Windows 2000 Server Security 3

Why the Change? 3

Differences in Windows 2000 Server Security 4

Authentication Limitations 7

What Is the Same in Windows 2000 Server? 9

Upgrading and Migrating Considerations 9

Network Security Plan 9

How to Begin the Process 11

Getting Started 12

Exercise 1.1 Switching to Native Mode 13

Issues to Present to Your Manager 15

Proper Analysis 16

Timing 16

Cost 16

Resources 17

Summary 18

Solutions Fast Track 18

Frequently Asked Questions 19

Chapter 2 Default Access Control Settings 21

Introduction 22

The Administrators Group 23

The Users Group 24

The Power Users Group 24

Configuring Security during Windows 2000 Setup 25
Default File System and Registry Permissions 30
Default User Rights 46
Exercise 2.1 Checking User Rights through the Microsoft Management Console 50
Default Group Membership 55
Pre-Windows 2000 Security 57
Summary 58
Solutions Fast Track 58
Frequently Asked Questions 60

Provides Details on the Subprotocols

Kerberos contains three subprotocols, also known as exchanges:

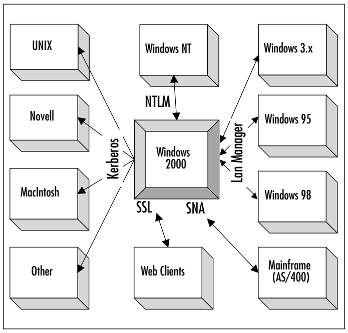
- Authentication Service (AS) Exchange
- Ticket-Granting Service (TGS) Exchange
- Client/Server (CS) Exchange

Chapter 3 Kerberos Server Authentication 63
Introduction 64
Authentication in Windows 2000 64
Benefits of Kerberos Authentication 66
Standards for Kerberos Authentication 66
Extensions to the Kerberos Protocol 67
Overview of the Kerberos Protocol 67
Basic Concepts 67
Authenticators 68
Key Distribution Center 69
Session Tickets 69
Ticket-Granting Tickets 71
Services Provided by the Key Distribution Center 72
Subprotocols 73
AS Exchange 73
TGS Exchange 75
CS Exchange 76
Option Flags for KRB_AS_REQ and KRB_TGS_REQ Messages 77
Tickets 78
Proxy Tickets and Forwarded Tickets 81
Kerberos and Windows 2000 82
Key Distribution Center 84

Kerberos Policy 86
Contents of a Microsoft Kerberos Ticket 88
Delegation of Authentication 88
Preauthentication 89
Security Support Providers 89
Credentials Cache 90
DNS Name Resolution 90
UDP and TCP Ports 91
Authorization Data 92
KDC and Authorization Data 92
Services and Authorization Data 92
Kerberos Tools 92
Kerberos List 93
Kerberos Tray 96
Summary 100
Solutions Fast Track 101
Frequently Asked Questions 103

Chapter 4 Secure Networking Using Windows 2000 Distributed Security Services 105
Introduction 106
The Way We Were: Security in NT 106
A Whole New World: Distributed Security in Windows 2000 106
Distributed Services 107
Open Standards 107
Windows 2000 Distributed Security Services 109
Active Directory and Security 110
Advantages of Active Directory Account Management 111
Managing Security via Object Properties 113
Managing Security via Group Memberships 115
Active Directory Object Permissions 115
Exercise 4.1 Assigning Active Directory Permissions to a Directory Object 116

Learn About Setting Up Secure Communication with Multiple Vendors via SSO



Relationship between Directory and Security Services 119
Active Directory Components 120
Exercise 4.2 Creating Trusts with Active Directory Domains and Trusts 126
Delegation of Administration 128
Fine-Grain Access Rights 131
Inheritance of Access Rights 131
Security Protocols 134
NTLM Credentials 134
Kerberos Credentials 135
Getting a Ticket to Ride 136
Private and Public Key Pairs and Certificates 137
Other Supported Protocols 137
Internet Single Sign-On 138
Internet Security for Windows 2000 139
Client Authentication with SSL 3.0 140
Authentication of External Users 140
Microsoft Certificate Server 140
CryptoAPI 141
Interbusiness Access: Distributed Partnership 141
Summary 143
Solutions Fast Track 144
Frequently Asked Questions 147

Chapter 5 Security Configuration Tool Set 149
Introduction 150
Security Configuration Tool Set 150
Security Configuration Tool Set Components 151
Security Configuration and Analysis Snap-In 151
Security Setting Extensions to Group Policy 151
Security Templates 152
The Secedit.exe Command-Line Tool 154
Security Configurations 154
Security Configuration and Analysis Database 154

Security Configuration and Analysis Areas 156
  Account Policies 157
  Local Policies 158
  Event Log 158
  Restricted Groups 158
  System Services 158
  Registry 158
  File System 158
Security Configuration Tool Set User Interfaces 159
  Security Configuration and Analysis Snap-In 159
  The Secedit.exe Command-Line Interface 161
Configuring Security 165
Account Policies 165
Local Policies 168
Event Log 174
Restricted Groups 176
  Exercise 5.1 Configuring Restricted Groups 177
Registry Security 179
  Exercise 5.2 Configuring Registry Security 179
File System Security 181
  Exercise 5.3 Configuring File System Security 181
System Services Security 184
  Exercise 5.4 Configuring System Services Security 185
Analyzing Security 186
  Exercise 5.5 Analyzing the Local Machine 186
Account and Local Policies 188
Restricted Group Management 188
Registry Security 188

Understand the Secedit.exe Command

The secedit.exe command-line interface allows the administrator to:

- Analyze system security
- Configure system security
- Refresh security settings
- Export security settings
- Validate the syntax of a security template

File System Security 189
System Services Security 190
Group Policy Integration 191
Security Configuration in Group Policy Objects 191
The Security Settings Extension to the Group Policy Editor 191
Additional Security Policies 193
Summary 194
Solutions Fast Track 195
Frequently Asked Questions 197

Learn the Syntax for the EfsRecvr Command Line

Item	Function
/S	Recovers the files in the given directory and all subdirectories. The default directory is the current directory.
/I	The recovery process will continue, even if an error occurs. The default behavior is to immediately stop the recovery process should an error occur.
/Q	Limits the reporting of only essential information needed to load the appropriate keys.
Filename	Specifies a file, directory, or pattern.

Chapter 6 Encrypting the File System for Windows 2000 199
Introduction 200
Using the Encrypting File System 201
Encryption Fundamentals 201
How EFS Works 203
User Operations 204
File Encryption 205
Assessing an Encrypted File 207
Copying an Encrypted File 208
The Copy Command 209
Moving or Renaming an Encrypted File 209
Decrypting a File 210
Cipher Utility 211
Directory Encryption 212
Recovery Operations 213
Exercise 6.1 Configuring a Recovery Agent without an EFS Certificate 213
Exercise 6.2 Adding a Recovery Agent That Has an EFS Recovery Certificate 218
EFS Architecture 221
EFS Components 222
The Encryption Process 224
The EFS File Information 227
The Decryption Process 229

Summary 232
Solutions Fast Track 233
Frequently Asked Questions 235

Chapter 7 IP Security for Microsoft Windows 2000 Server 239
Introduction 240
Network Encroachment Methodologies 240
Snooping 241
Spoofing 241
The TCP/IP Sequence Number Attack 241
Password Compromise 242
Denial-of-Service Attacks 242
TCP SYN Attacks 243
SMURF Attacks 243
Teardrop Attacks 244
Ping of Death 244
Man-in-the-Middle Attacks 244
Application-Directed Attacks 245
Compromised Key Attacks 245
IPSec Architecture 246
Overview of IPSec Cryptographic Services 247
Message Integrity 247
Message Authentication 249
Confidentiality 251
IPSec Security Services 252
The Authentication Header 252
Encapsulating Security Payload 253
Security Associations and IPSec Key Management Procedures 254
IPSec Key Management 255
Deploying Windows IP Security 256
Evaluating Information 256
Evaluating the "Enemy" 257
Determining Required Security Levels 258
Building Security Policies with Customized IPSec Consoles 259

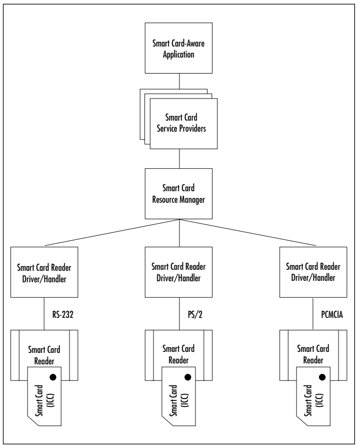
Implement IPSec Security Services

IPSec engages two protocols to implement security on an IP network:

- Authentication header (AH)
- Encapsulating security protocol (ESP)

Exercise 7.1 Building an IPSec MMC Console 259
Flexible Security Policies 261
Rules 263
Flexible Negotiation Policies 267
Filters 268
Creating a Security Policy 269
Making the Rule 271
Compatibility Notes 283
Summary 284
Solutions Fast Track 285
Frequently Asked Questions 287

Learn About the Interaction between a Smart Card Application and a Smart Card Reader


Smart Card-Aware Application
Smart Card Service Providers
Smart Card Resource Manager
Smart Card Reader Driver/Handler
Smart Card Reader Driver/Handler
Smart Card Reader Driver/Handler
RS-232
PS/2
PCMCIA
Smart Card Reader
Smart Card Reader
Smart Card Reader
Smart Card (ICC)
Smart Card (ICC)
Smart Card (ICC)

Chapter 8 Smart Cards 289
Introduction 290
Interoperability 291
ISO 7816, EMV, and GSM 291
The PC/SC Workgroup 292
The Microsoft Approach 292
A Standard Model for Interfacing Smart Card Readers and Cards with PCs 293
Device-Independent APIs for Enabling Smart Card-Aware Applications 294
Integration with Various Microsoft Platforms 295
Smart Card Base Components 296
Service Providers 296
Cryptographic Service Providers 296
Smart Card Service Providers 296
Cards 297
Resource Manager 300
Enhanced Solutions 302
Client Authentication 302
Public Key Interactive Logon 302
Smart Card Reader Installation 303
Smart Card Certificate Enrollment 305
Smart Card Logon 309

Secure E-Mail 309
Summary 311
Solutions Fast Track 311
Frequently Asked Questions 313

Chapter 9 Microsoft Windows 2000 Public Key Infrastructure 315
Introduction 316
Concepts 316
Public Key Cryptography 317
Public Key Functionality 319
Digital Signatures 319
Authentication 321
Secret Key Agreement via Public Key 322
Bulk Data Encryption without Prior Shared Secrets 322
Protecting and Trusting Cryptographic Keys 323
Certificates 323
Certificate Authorities 324
Certificate Types 325
Trust and Validation 326
Windows 2000 PKI Components 328
Certificate Authorities 329
Certificate Hierarchies 330
Deploying an Enterprise CA 331
Trust in Multiple CA Hierarchies 332
Installing a Windows 2000 PKI 333
Exercise 9.1 Installing Certificate Services 334
Enabling Domain Clients 338
Generating Keys 338
Key Recovery 338
Exercise 9.2 Exporting a Certificate and a Private Key 339
Certificate Enrollment 343

Learn About Why Certificates Can Be Revoked

Any of these circumstances would certainly warrant the revoking of a certificate:

- An entity's private key has been compromised.
- A project with another organization is completed.
- The employee has changed status within the company.
- A department is to cease having access to certain information.
- The certificate was obtained through forgery.

Exercise 9.3 Requesting a User Certificate with the Certificate Request Wizard 343
Exercise 9.4 Requesting an EFS Recovery Agent Certificate from the CA Web Page 348
Renewal 352
Using Keys and Certificates 352
Roaming 353
Revocation 354
Exercise 9.5 Revoking a Certificate and Publishing a CRL 355
Trust 356
Exercise 9.6 Importing a Certificate from a Trusted Root CA 357
Public Key Security Policy in Windows 2000 361
Trusted CA Roots 361
Exercise 9.7 Configuring Automatic Certificate Enrollment through Group Policy 363
Certificate Enrollment and Renewal 366
Exercise 9.8 Changing the Templates Available on the Enterprise Certification Authority 368
Smart Card Logon 369
Applications Overview 369
Web Security 370
Secure E-Mail 370
Digitally Signed Content 371
Encrypting File System 373
Smart-Card Logon 373
IP Security 374
Preparing for Windows 2000 PKI 375
Backing Up and Restoring Certificate Services 377
Exercise 9.9 Backing Up Certificate Services 377

Exercise 9.10 Restoring Certificate Services 379
Summary 383
Solutions Fast Track 385
Frequently Asked Questions 389

Chapter 10 Supporting Non-Windows 2000 Clients and Servers 393

Introduction 394
Authenticating Down-Level Clients 394
Defining Lan Manager and NT Lan Manager Authentication 395
Using the Directory Services Client 396
Deploying NTLM Version 2 397
Configuring the Servers to Require NTLMv2 397
Making the Clients Use NTLMv2 400
Exercise 10.1 Configuring Windows NT 4.0 Clients to Use NTLMv2 400
Exercise 10.2 Configuring Windows 9x Clients to Use NTLMv2 401
Working with UNIX Clients 402
Installing Services for UNIX 403
Exercise 10.3 Adding a User to the Schema Admin Group 404
Exercise 10.4 Enabling the Schema Master for Write Operation 406
Exercise 10.5 Installing Services for UNIX 411
NFS Software 418
Using the Client Software for NFS 418
Using the Server Software for NFS 420
Using the Gateway Software for NFS 422
Using the PCNFS Server Software for NFS 422
Account Administration Tools 424
Network Administration Tools 432

Authenticating Down-Level Clients

Microsoft considers all clients running any Microsoft operating system (OS) other than Windows 2000 to be *down-level clients*. In Chapter 10, we focus on the following operating systems:

- Windows 95
- Windows 98
- Windows NT 4.0

Using the UNIX Utilities 435
Authenticating UNIX Clients 438
Working with Novell Clients 439
Client Services for NetWare 441
Gateway Services for NetWare 441
Exercise 10.6 Installing Gateway Services for NetWare 442
Exercise 10.7 Configuring Gateway Services for NetWare 445
Understanding Services for NetWare 447
Exercise 10.8 Installing Services for NetWare 447
Using Microsoft Directory Synchronization Services 452
Using the Microsoft File Migration Utility 453
Using File and Print Services for NetWare 460
Understanding the Security Risk Associated With Accessing NetWare Computers 460
Working with Macintosh Clients 462
Understanding Files Services for Macintosh 462
Understanding Print Services for Macintosh 463
Installing File and Print Services for Macintosh 463
Authenticating Macintosh Clients 464
Summary 465
Solutions Fast Track 467
Frequently Asked Questions 468

Chapter 11 Securing Internet Information Services 5.0 471

Introduction 472
Securing the Windows 2000 Server 473
Installing Internet Information Services 5.0 475

Exercise 11.1 Uninstalling IIS 5.0 476
Exercise 11.2 Creating an Answer File for Installing IIS 480
Securing Internet Information Services 5.0 481
Setting Web Site, FTP Site, and Folder Permissions 481
Configuring Web Site Permissions 482
Configure FTP Site Permissions 484
Exercise 11.3 Setting FTP Site Permissions 485
Configuring NTFS Permissions 485
Using the Permissions Wizard 487
Using the Permission Wizard Template Maker 490
Restricting Access through IP Address and Domain Name Blocking 495
Configuring Authentication 497
Configuring Web Site Authentication 505
Exercise 11.4 Selecting the Level of Authentication Supported 505
Configuring FTP Site Authentication 509
Exercise 11.5 Setting FTP Authentication 510
Examining the IIS Security Tools 511
Using the Hotfix Checking Tool for IIS 5.0 511
Using the IIS Security Planning Tool 513
Using the Windows 2000 Internet Server Security Configuration Tool for IIS 5.0 514
The Interviewing Process 515
Configuring the Template Files 515
Deploying the Template Files 524
Auditing IIS 526
Exercise 11.6 Configuring Auditing for an Organizational Unit 527
Summary 529
Solutions Fast Track 530
Frequently Asked Questions 533

Learn the NTFS Permissions

- Full Control
- Modify
- Read and Execute
- List Folder Contents
- Read
- Write

Chapter 12 Using Security-Related Tools 535

Introduction 536
Installing the Support Tools 536
Exercise 12.1 Installing the Support Tools 537
Installing the Windows 2000 Server Resource Kit 540
Exercise 12.2 Installing the Windows 2000 Server Resource Kit 540
Using Application Tools 544
Using the Application Security Tool 545
Installing the Application Security Tool 546
Running the Applications as Services Utility 546
Installing Srvany 547
Exercise 12.3 Using Srvany 547
Exercise 12.4 Using the Service Installation Wizard 547
Configuring an Application to Run as a Service 552
Exercise 12.5 Configuring the Registry to Run Applications as Services 553
Using Service Tools 556
Running the Service Controller Tool 556
Using ScList 558
Using the Service Monitoring Tool 561
Exercise 12.6 Running the Service Monitor Configuration Wizard 561
Using Registry Tools 564
Using Registry Backup 564
Using Registry Restoration 565
Running the Registry Console Tool 566
Using Process Tools 569
Running the Process Viewer 570
Running the Task List Viewer 571
Using the Task Killing Utility 573
Using Process Tree 573
Exercise 12.7 Installing Process Tree 575

Use the Service Monitoring Tool

The Service Monitoring tool (**svcmon**) monitors when services are started or stopped. Svcmon works locally and remotely. It will send you an e-mail when a service is changed. Svcmon polls the services every 10 minutes to determine that they are in the same state as they were in the previous poll.

Using PuList 579
Using Logging Tools 581
Using the Event Log Query Tool 582
Using Trace Logging 582
Using Trace Dump 585
Using Reduce Trace Data 587
Using Permission Tools 588
Using the Service ACL Editor 589
Using Permcopy 590
Running Access Control List Diagnostics 590
Running DsAcls 591
Using Group Management Tools 593
Show Groups 594
Using Show Members 594
Using Find Group 595
Using Miscellaneous Tools 595
Using Show Privilege 595
Running Uptime 597
Heartbeat 598
Using Floppy Lock 601
Running System Scanner 602
Exercise 12.8 Installing System Scanner 1.1 602
Exercise 12.9 Running a Scan with System Scanner 608
Summary 612
Solutions Fast Track 612
Frequently Asked Questions 615

Appendix A Port Numbers 617

Index 653