SYNGRESS®

4 FREE BOOKLETS

YOUR SOLUTIONS MEMBERSHIP

SYNGRESS 4 FREE E-BOOKLETS PUBLISHING

Windows Linux Migration Toolkit

Your Windows to Linux Extreme Makeover!

- Fully Functioning Scripts on CD-ROM Automate Your Migration Tasks
- Complete Coverage of Migration Process Planning, Anti-Virus and Anti-Spam Applications, and Deployment Details
- Covers Windows 95; 98, 98SE, and Me; NT4; Windows 2000; and Windows XP. Applies to ALL Linux Distributions.

David Allen

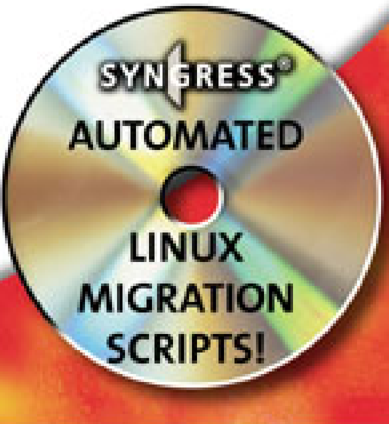
Andrew Scott

Herb Lewis

John Stile

Tim Tuck

Christian Lahti Technical Editor



Register for Free Membership to

solutions@syngress.com

Over the last few years, Syngress has published many best-selling and critically acclaimed books, including Tom Shinder's *Configuring ISA Server 2000*, Brian Caswell and Jay Beale's *Snort 2.0 Intrusion Detection*, and Angela Orebaugh and Gilbert Ramirez's *Ethereal Packet Sniffing*. One of the reasons for the success of these books has been our unique **solutions@syngress.com** program. Through this site, we've been able to provide readers a real time extension to the printed book.

As a registered owner of this book, you will qualify for free access to our members-only solutions@syngress.com program. Once you have registered, you will enjoy several benefits, including:

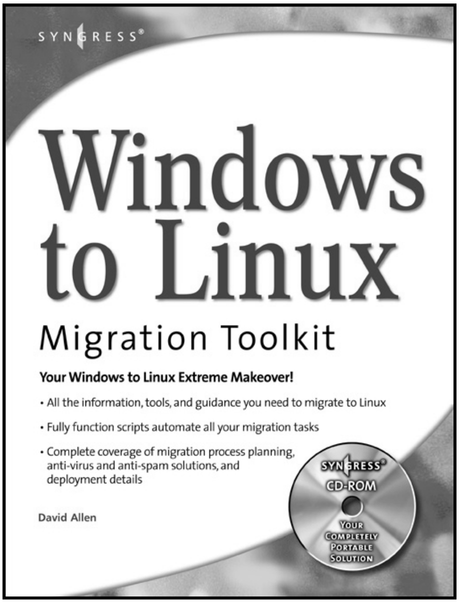
- Four downloadable e-booklets on topics related to the book. Each booklet is approximately 20-30 pages in Adobe PDF format. They have been selected by our editors from other best-selling Syngress books as providing topic coverage that is directly related to the coverage in this book.
- A comprehensive FAQ page that consolidates all of the key points of this book into an easy to search web page, providing you with the concise, easy to access data you need to perform your job.
- A "From the Author" Forum that allows the authors of this book to post timely updates links to related sites, or additional topic coverage that may have been requested by readers.

Just visit us at **www.syngress.com/solutions** and follow the simple registration process. You will need to have this book with you when you register.

Thank you for giving us the opportunity to serve your needs. And be sure to let us know if there is anything else we can do to make your job easier.

SYNGRESS®

Computer Resources Consulting, Inc.
http://www.crconsulting.com (800) 884-9885



SYNGRESS®

Windows to Linux

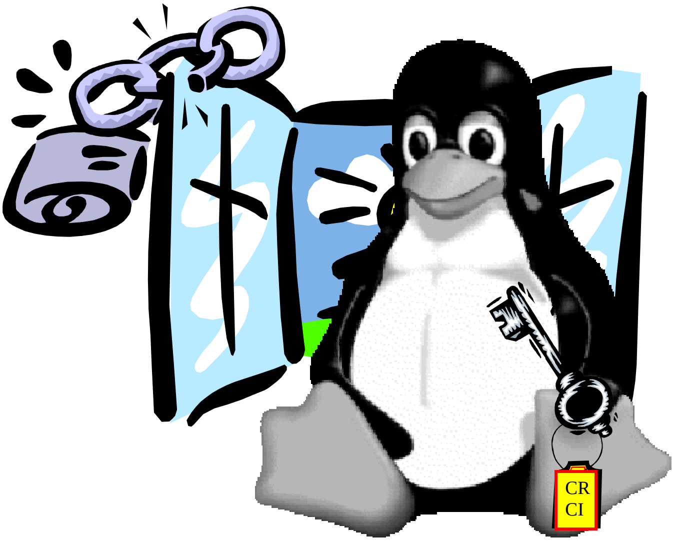
Migration Toolkit

Your Windows to Linux Extreme Makeover!

- All the information, tools, and guidance you need to migrate to Linux
- Fully function scripts automate all your migration tasks
- Complete coverage of migration process planning, anti-virus and anti-spam solutions, and deployment details

David Allen

SYNGRESS® CD-ROM Your Completely Portable Solution



The authors of this breakthrough book are available for consulting, support and training in migrating, networking, security, and systems. With over 25,000 successful migrations on five continents, Computer Resources Consulting has the expertise to ensure a smooth migration to systems that deliver outstanding value and increased productivity to any company. CR Consulting's satisfied clients include JPMorgan Chase, Charles Schwab, Credit Suisse First Boston, Applied Materials, NASA, and dozens of small businesses.

RELIABILITY * SCALABILITY * 24 x 7 AVAILABILITY

E-Mail	MigrationHelp@crconsulting.com
On the Web	http://www.crconsulting.com
By Telephone	(800) 884-9985

CR Consulting
Incorporated

SYNGRESS®

Windows to Linux

Migration Toolkit

David Allen

Andrew Scott

Herb Lewis

John Stile

Tim Tuck

Christian Lahti Technical Editor

Syngress Publishing, Inc., the author(s), and any person or firm involved in the writing, editing, or production (collectively "Makers") of this book ("the Work") do not guarantee or warrant the results to be obtained from the Work.

There is no guarantee of any kind, expressed or implied, regarding the Work or its contents. The Work is sold AS IS and WITHOUT WARRANTY. You may have other legal rights, which vary from state to state.

In no event will Makers be liable to you for damages, including any loss of profits, lost savings, or other incidental or consequential damages arising out from the Work or its contents. Because some states do not allow the exclusion or limitation of liability for consequential or incidental damages, the above limitation may not apply to you.

You should always use reasonable care, including backup and other appropriate precautions, when working with computers, networks, data, and files.

Syngress Media®, Syngress®, "Career Advancement Through Skill Enhancement®," "Ask the Author UPDATE®," and "Hack Proofing®," are registered trademarks of Syngress Publishing, Inc. "Syngress: The Definition of a Serious Security Library"™, "Mission Critical™," and "The Only Way to Stop a Hacker is to Think Like One™" are trademarks of Syngress Publishing, Inc. Brands and product names mentioned in this book are trademarks or service marks of their respective companies.

KEY	**SERIAL NUMBER**
001	HJIR78N764
002	PO987JNHFG
003	82NJH24562
004	CVPLQ6WQ23
005	JKNN6653FL
006	VBT5GHFF42
007	HJJEVBNK98
008	29WMKGHGG8
009	629TGHVB56
010	IMTVCX32X4

PUBLISHED BY
Syngress Publishing, Inc.
800 Hingham Street
Rockland, MA 02370

Windows to Linux Migration Toolkit

Copyright © 2004 by Syngress Publishing, Inc. All rights reserved. Printed in the United States of America. Except as permitted under the Copyright Act of 1976, no part of this publication may be reproduced or distributed in any form or by any means, or stored in a database or retrieval system, without the prior written permission of the publisher, with the exception that the program listings may be entered, stored, and executed in a computer system, but they may not be reproduced for publication.

Printed in the United States of America
1 2 3 4 5 6 7 8 9 0
ISBN: 1-931836-39-6

Publisher: Andrew Williams
Acquisitions Editor: Jaime Quigley
Technical Editor: Christian Lahti and David Allen
Cover Designer: Michael Kavish

Page Layout and Art: Patricia Lupien
Copy Editor: Amy Thomson
Indexer: Rich Carlson

Distributed by O'Reilly Media, Inc. in the United States and Canada.
For information on rights and translations, contact Matt Pedersen, Director of Sales and Rights, at Syngress Publishing; email matt@syngress.com or fax to 781-681-3585.

Acknowledgments

Syngress would like to acknowledge the following people for their kindness and support in making this book possible.

Syngress books are now distributed in the United States and Canada by O'Reilly Media, Inc.The enthusiasm and work ethic at O'Reilly is incredible and we would like to thank everyone there for their time and efforts to bring Syngress books to market:Tim O'Reilly, Laura Baldwin, Mark Brokering, Mike Leonard, Donna Selenko, Bonnie Sheehan, Cindy Davis, Grant Kikkert, Opol Matsutaro, Steve Hazelwood, Mark Wilson, Rick Brown, Leslie Becker, Jill Lothrop,Tim Hinton, Kyle Hart, Sara Winge, C. J. Rayhill, Peter Pardo, Leslie Crandell, Valerie Dow, Regina Aggio, Pascal Honscher, Preston Paull, Susan Thompson, Bruce Stewart, Laura Schmier, Sue Willing, Mark Jacobsen, Betsy Waliszewski, Dawn Mann, Kathryn Barrett, John Chodacki, and Rob Bullington.

The incredibly hard working team at Elsevier Science, including Jonathan Bunkell, Ian Seager, Duncan Enright, David Burton, Rosanna Ramacciotti, Robert Fairbrother, Miguel Sanchez, Klaus Beran, Emma Wyatt, Rosie Moss, Chris Hossack, Mark Hunt, and Krista Leppiko, for making certain that our vision remains worldwide in scope.

David Buckland, Marie Chieng, Lucy Chong, Leslie Lim, Audrey Gan, Pang Ai Hua, and Joseph Chan of STP Distributors for the enthusiasm with which they receive our books.

Kwon Sung June at Acorn Publishing for his support.

David Scott, Tricia Wilden, Marilla Burgess, Annette Scott, Andrew Swaffer, Stephen O'Donoghue, Bec Lowe, and Mark Langley of Woodslane for distributing our books throughout Australia, New Zealand, Papua New Guinea, Fiji Tonga, Solomon Islands, and the Cook Islands.

Winston Lim of Global Publishing for his help and support with distribution of Syngress books in the Philippines.

Lead Author

David Allen (President, CRCI) is the lead author and technical editor of *Windows to Linux Migration Toolkit*. David started programming computers when he was eight years old, and has over two decades of experience in the computer field. David has been responsible for over 25,000 migrations on five continents. He has worked for international banks (Schwab, Credit Suisse, JPMorgan), technology companies, and government organizations including NASA. David has been an Open Source advocate for many years, and is a speaker at LinuxWorld and O'Reilly's Open Source Convention.

David founded Computer Resources Consulting, Inc. to provide consulting services to clients around the world. CRCI provides migration, support, training, and security consulting using open source solutions. For more information about CRCI and migration services provided by the authors of this book, navigate to www.crconsulting.com or phone (800) 884-9885.

Contributing Authors

Herbert Lewis has been a member of the Samba team since 1997. He currently works at Panasas Inc. where he helps to support the CIFS gateway portion of the product using Samba software. He previously worked at SGI developing and maintaining the Samba software, as well as several other open-source software products on the IRIX operating system. He holds a bachelor's degree from the U.S. Coast Guard Academy, as well as a master's degree and an engineer's degree from Stanford University.

John Streeton Stile is the Senior Technical Engineer for Pervasive Netwerks, designing Open Source solutions for Windows and Unix environments. With his bachelor of science in biochemistry from the University of California, Davis, and drug discover R&D experience, John applies the scientific method to research, engineering, and trouble shooting network and computer solutions.

John joined the computer industry in 1997, and began exploring Unix in 1999 after discovering that, unlike biology, there is always a solution to computer problems. He has worked with entities large and small, public and private, in various industries, including: Industrial Light and Magic, Adobe Systems, Ohlone College, Certicom, and Skyflow.

John would like to thank John H. Terpstra for offering advice, updating RPMs, and adding a personal touch during the writing of this book. John is the author of *Samba-3 By Example,* the soon-to-be-released *OpenLDAP By Example,* and is a contractor for Samba solutions.

James Stanger (PhD., CIW Master Administrator, Linux+, Security+, A+, CTP) is Vice President of Certification at ProsoftTraining. He is chair of the LPI Advisory Council, leads CIW exam development, and has helped developed certifications for Symantec and CompTIA. A prolific author, James has created titles for ComputerPREP, Symantec, Syngress, Sybex, and McGraw Hill. His titles include *Hack Proofing Linux*, the *E-mail Virus Protection Handbook*, and *Advanced Internet Services Management.* He is also an accomplished network consultant, where he specializes in security auditing, Windows to Linux migration, and LAMP-based e-commerce solutions.

Andrew Taylor Scott is a student of computer science and philosophy at City College of San Francisco and part-time Linux consultant for non-profits looking to leverage open source software within their organizations. Before he went back to school, he was working at Linuxcare Inc., a revolutionary organization providing distribution-neutral technical support and professional services to enterprise-level companies seeking Linux solutions. While at Linuxcare, Andrew held the positions of Technical Support Engineer, Professional Services Consultant. He also served as Technical Writer, developing courseware in SGML for training Linux engineers in email systems and Web systems hosted on GNU/Linux. Taking full advantage of his time at Linuxcare, he learned as much as he could about GNU/Linux and the Free Software movement by involving himself in the development and release of several versions of the Linuxcare Bootable Business Card and the LNX-BBC mini-Linux distributions. He has since served as a consultant on several custom Linux solutions developing Web applications with Linux, Apache, MySQL, and PHP (LAMP).

Some of Andrew's clients include Thrasher Magazine, Theme-Co-op Promotions®, Fast Country, Institute for Collaborative Change, and Associated Students Councils at CCSF. He has completed several certifications in Linux system and network administration from Linuxcare University, including LNX-102, LNX-201, LNX-202, and LNX-301. He has also received Sun's Solaris System Administration I certification and has excelled in multiple in-depth classes regarding Unix and Linux operating system internals and C++ programming. Andrew has real-world experience deploying Linux servers for in-house networks, as well as collocated networks, establishing hardware and network needs, and designing appropriate Linux fixtures—often at a greatly reduced cost compared to commercial solutions. He is currently working on developing open source groupware with LAMP for virtual hosts.

Timothy Tuck is the President of Pervasive Netwerks and the Founder of the Hayward Linux Users group known as LinuxDojo.net. He specializes in Linux and Windows to Linux migrations. His company currently provides IT services for over 70 Companies in and around the Silicon Valley. Timothy's background includes positions in research and development as a Prototyper for Logitech, and as a Senior Engineering Tech and Lab Administrator at Cisco Systems. He has been working with computers for the last

20 years, using Linux on the desktop for the last 6 years. Timothy currently resides in Hayward, CA and is married to the most wonderful woman in the world, Louise Cheng.

Timothy would like to give special mentions and thanks to David Allen for coming up with the idea for this book, Jaime Quigley for her help during the writing process, Andrew Scott for his help during the editing of chapters, and to Rick Moen for the recommendation. A huge ‘thank you’ goes out to all of the hackers and programmers who contribute to Open Source Software. Their contributions have made all of this possible. To Linus Torvalds for giving the world the ultimate gift, Linux; the gift that keeps on giving. To the penguinheads from LinuxDojo.net, whose contributions to the users group keep it fun and real month after month. Special mention to Tim’s lovely wife, who has given up everything to come half way across the world to put up with his endless hours of hacking around.

Technical Editor

Christian Lahti is a senior consultant with CRCI and has over 15 years experience in the IT industry. He is an expert in security, systems, and networking, having developed and implemented global IT infrastructures with a focus on Linux and open source, as well as providing consulting expertise for successful cross-platform integrations and interoperability. In addition, he is also skilled in database design as well as web development. Christian is a speaker and tutorial presenter at both LinuxWorld and O’Reilly’s OSCON.

Contents

About the CD xxv

Foreword xxix

Chapter 1 Network Services Migration Roadmap 1

- Introduction 2
- Assessing the Current Infrastructure 2
    - A Tale of Two Companies 3
    - Inventorying the Servers 5
    - Creating an Infrastructure Diagram 6
    - Documenting Additional Assessment Information 8
- Determining Requirements for the Linux Infrastructure 8
    - Creating a Functional Requirements Document 8
    - Identifying Constraints 10
- Designing the Linux Infrastructure 11
    - Creating a Post-Migration Infrastructure Design 11
- Testing the Linux Infrastructure 13
    - Creating a Test Plan 14
- Deploying the Linux Infrastructure 16
- Migrating to the Linux Infrastructure 16
- Summary 18
- Solutions Fast Track 18

Chapter 2 Core TCP/IP Networking Services 21

- Introduction 22
- Understanding IP Address Assignment Services 23
    - Understanding DHCP Clients 24
        - Obtaining the Initial DHCP Lease 24
        - Renewing a DHCP Lease 26
        - Releasing a DHCP Lease 27

Configuring DHCP Servers 28
Understanding Name Resolution Services 31
Understanding File-Based Name Resolution 31
Understanding DNS Name Resolution 32
Understanding Dynamic DNS (DDNS) 33
Configuring BIND and DHCP for Dynamic DNS 33
Understanding Time Synchronization Services 34
Understanding Network Time Protocol 34
Understanding Linux NTP Clients 35
Understanding Windows Time Service Clients 36
Migrating MS-DNS/DHCP to Linux BIND/DHCPD . . .37
Migrating the DHCP Scopes and Options 38
Determining the DHCP Scopes and Options on Windows NT 38
Determining the DHCP Scopes and Options on Windows 2000 39
Recording the DHCP Scopes and Options 40
Configuring the ISC DHCPD Server 41
Migrating from Microsoft DHCP Services to Linux DHCP Services 42
Backing Out of a Failed DHCP Migration 42
Migrating the DNS Information 42
Installing and Configuring BIND 42
Transferring DNS Information 43
Migrating from Microsoft DNS Services to Linux DNS Services 44
Backing Out of a Failed DNS Migration 45
Summary 46
Solutions Fast Track 46
Frequently Asked Questions 49

Chapter 3 Directory Services .51
Introduction 52
Understanding LDAP and Directories 52
Understanding LDAP Terms .53
Understanding Directory Structure 53
Understanding Directory Objects 54

Connecting to a Directory Server 55
Understanding LDAP Queries .56
Understanding Microsoft Directory Services 57
Understanding Windows NT SAM 57
Understanding Exchange 5.5 Directory Services 58
Understanding Active Directory 58
Understanding OpenLDAP 59
Understanding OpenLDAP Server Daemons 60
Understanding OpenLDAP Utilities 60
Designing Linux-Based Directory Services 61
Designing a Directory Information Tree 61
Designing the OpenLDAP Infrastructure 62
Configuring and Testing the OpenLDAP Server(s) 64
Summary 67
Solutions Fast Track 67
Frequently Asked Questions 70

Chapter 4 Authentication Services 71
Introduction 72
Understanding Windows Authentication 73
Understanding Windows 98/NT Logon 73
Understanding Windows 2000/XP Logon 74
Understanding Linux Authentication 74
Understanding LDAP Authentication 75
Understanding /etc/passwd/shadow Authentication . . .76
Understanding NIS Authentication 77
Understanding Linux Client Authentication Settings . . .77
Understanding Name Service Switch (nsswitch.conf) 77
Understanding LDAP Configuration Settings (ldap.conf) 78
Understanding PAM 79
Designing Linux-Based Authentication Services 81
Designing Cross-Platform Authentication Services 82
Installing and Configuring Samba 84
Migrating from NT/Exchange or Active Directory 88
Preparing for Migration 88
NT / Exchange 5.5 Migration Path 89

Active Directory Migration Path 93
Migrating Windows Logon Authentication Files 97
Testing Authentication Services 97
Enabling Encryption 97
Summary 100
Solutions Fast Track 100
Frequently Asked Questions 103

Chapter 5 File Services 105
Introduction 106
Understanding Windows File Systems 106
Understanding Windows File Allocation Table File Systems 106
Understanding Windows NTFS File Systems 109
Understanding Linux File Systems 112
Understanding Ext2/3 113
Resources 114
Understanding ReiserFS 115
Resources 116
Understanding Permissions Management (Access Control) 118
Understanding File Backup, Restore, and Replication Options 123
Identify Critical Files to be Backed Up 124
Decide on a Backup Method 125
Determine What Type of Backup Media to Use . . .125
Backup Schedules 126
Plan to Rotate and Archive Media 127
AMANDA 129
AMANDA Backup Process .130
Installing AMANDA 132
On the Server 134
On Linux Clients 137
For Windows Clients 138
Set Up a Backup on the Server 138
Designing Linux-based File Services 139
Hardware Resources 139
Migrating File Services to Linux 140

Migrating the File Permissions 142
Support Tools Utility showwaccs 144
Solutions Fast Track 145
Understanding Linux File Systems 145
Understanding Permissions Management (Access Control) 145
Understanding File Backup, Restore, and Replication Options 146
AMANDA 146
Frequently Asked Questions 147

Chapter 6 Print Services 149
Introduction 150
Understanding Windows Print Services 150
Understanding Linux Print Services 151
Configuring Linux Printing Using BSD or SYSV 153
Configuring Linux Printing Using CUPS 155
Sharing Samba Printers 161
Understanding Automatic Printer Driver Downloading . . .170
Migrating Windows Print Services to CUPS/Samba 175
Summary 176
Solutions Fast Track 176
Frequently Asked Questions 178

Chapter 7 Messaging Services 181
Introduction 182
Understanding Microsoft Messaging Services 183
Understanding Exchange 5.5 Messaging 184
Understanding Exchange 2000 Messaging 186
Understanding Linux-Based Messaging Services 187
Sending and Receiving Internet E-mail 187
Understanding Linux Messaging System Components .189
Mail User Agent 190
Mail Access Agent (MAA) 192
Mail Transfer Agent (MTA) 193
Mail Delivery Agent 195
Mailstore 195

Exploring Open Source Messaging Server Software . . .197
Sendmail 197
Qmail 198
Postfix 199
Exim 200
Courier Suite 200
Designing Linux-Based Messaging Services 205
Determining the Internet E-mail Architecture 205
Choosing Messaging Server Software 208
Determining How to Store the E-mail 210
Creating a Linux E-mail Server Diagram 211
Integrating Anti-Spam and Anti-Virus Services 212
Understanding Spam 213
Determining if an E-Mail is Spam 213
Whitelisting and Blacklisting 216
Understanding Viruses 216
Exploring Open Source Anti-Spam / Anti-Virus Applications 219
SpamAssassin 220
Clam AntiVirus 220
MailScanner 221
Designing Anti-Spam / Anti-Virus Services 221
Shared E-Mail / Anti-Spam / Anti-Virus Server Option 222
Dedicated Anti-Spam / Anti-Virus Gateway Option 222
Commercial Appliance Option 224
Outsourced Option 224
Migrating Information from Exchange to Linux 225
Preparing Exchange for Migration 225
Installing the Courier IMAP server suite 227
Migrating E-mail to Linux 228
Summary 230
Solutions Fast Track 231
Frequently Asked Questions .234

Chapter 8 Groupware and Calendaring Services 235
Introduction 236
Understanding Exchange and Outlook Groupware and Calendaring Features 236
Understanding Linux-Based Groupware and Calendaring Services 238
Understanding eGroupware 238
Understanding Horde 239
Reviewing OPEN-XCHANGE (OX) 240
Understanding TWiki Collaboration 241
Migrating to Linux Groupware / Calendaring Services . . .242
Understanding Outport 243
Understanding Other Migration Methodologies 244
Summary 245
Solutions Fast Track 245
Frequently Asked Questions 247

Chapter 9 Web Services: IIS vs Apache 249
Introduction 250
Background: HyperText Transfer Protocol 251
Understanding Microsoft's Internet Information Server . . .252
Getting Started 252
Default Index Page 253
Default Web Site 255
Virtual Directories 256
Security 257
SSL/TLS 258
Virtual Servers 260
Understanding Apache Web Server 262
Background of Apache 263
Installation 264
Starting, Stopping, and Checking Status 264
Configuration 265
Basic Configuration Options for the Main Server . .267
Default Web Page 270
Aliases and ScriptAliases 271
Security and Permissions 272

.htaccess Files 275
Virtual Hosting 276
Modules 282
Graphical Tools 284
Migrating Static Sites from IIS to Apache 286
Summary 287
Solutions Fast Track 287
Frequently Asked Questions .289

Chapter 10 Desktop Migration Roadmap 291
Introduction 292
Assessing the Current Desktop Environment 294
User Types 294
Kiosk 294
Basic Knowledge Worker 294
Transactional Worker 295
Technical Worker 295
Advanced Knowledge Worker 295
Creating the Desktop Asset List 295
Cataloging File Formats 299
Functional Requirement Specification 300
Designing the Linux Desktop .301
Functional Replacement Specification 303
Building the Training Computers 304
Testing the Linux Desktop 305
Migrating Application Data and Profiles 305
Backing Up Desktop Systems 306
Installing Linux 307
Importing User Profiles and Preferences 307
Training the Desktop Users 307
Training Guidelines 308
Linux Desktop Differences .309
Filesystem Differences 310
Other Differences 310
Alternative Application Equivalents 311
Getting Help 312
Deploying the Linux Desktops 312

Documentation 313
Summary 314
Solutions Fast Track 314
Frequently Asked Questions 316

Chapter 11 Inside the Typical Linux Desktop 317
Introduction 318
Common Desktop Environments .318
Gnome 319
KDE 321
Common Features 323
Install Both, Make One the Default 323
Alternative Window Managers 323
The X Window System and Window Managers 324
X Window Servers versus Window Managers 325
Window Managers as Alternative Desktop Environments 327
E-Mail and Personal Information Management Clients . . .329
Evolution 330
Evolution, Microsoft Exchange, Novell GroupWise, and OpenExchange 332
KDE Suite/KMail 332
Kontact 333
Aethera 333
Mozilla Mail/Thunderbird 334
Thunderbird 335
Sylpheed 335
Essential Information 336
Recommending E-Mail and PIM Software 336
Migrating Mail 337
Migrating from Outlook or Outlook Express 337
Importing Outlook Mail into Mozilla 338
LibPST 339
Importing Outlook Mail into Evolution 339
Document Standards 342
The Hard Way 342
Web Browsers 342

Mozilla 343
Mozilla and Microsoft CHAP 344
Firefox 344
Galeon 345
Konqueror 346
Opera 346
Migrating Bookmarks 347
Browser Plug-Ins 347
Macromedia Flash and Shockwave/Director 348
RealPlayer 348
Adobe Acrobat Reader 349
Office Application Suites .350
OpenOffice.org 351
Limitations: Macros and PDF Files 353
Future Plans 354
StarOffice 354
KOffice 355
Hancom Office 355
Running Windows Applications on Linux 356
Compatibility Layer Software 356
Wine 357
Code Weavers' CrossOver Office 358
Summary 359
Solutions Fast Track 359
Frequently Asked Questions .361

Appendix A Introducing Network Analysis and Ethereal 365

Introduction 366
What is Network Analysis and Sniffing? 366
Who Uses Network Analysis? .369
How are Intruders Using Sniffers? 370
What does Sniffed Data Look Like? 372
Common Network Analyzers 373
How Does It Work? 378
Explaining Ethernet 378
Understanding the OSI model 380

CSMA/CD 384
Hardware: Taps, Hubs, and Switches, Oh My! 385
Port Mirroring 388
Defeating Switches 389
Detecting Sniffers 391
Protecting Against Sniffers 395
Network Analysis and Policy .397
Summary 398
Solutions Fast Track 399
Frequently Asked Questions 401
Appendix B Introducing Intrusion Detection Systems and Snort 403
Introducing Intrusion Detection Systems 404
What Is an Intrusion? 404
Legal Definitions 405
Scanning vs. Compromise 407
Viruses and Worms—SQL Slammer 408
Live Attacks—Sendmail Buffer Overflow 411
How an IDS Works 411
What the IDS Is Watching 411
How the IDS Watches Your Network 422
How the IDS Takes the Data It Gathers and Finds Intrusion Attempts 424
What the IDS Does When It Finds an Attack Attempt 427
Answering Common IDS Questions 429
Why Are Intrusion Detection Systems Important? . . .430
Why Doesn't My Firewall Serve as an IDS? 430
Why Are Attackers Interested in Me? 430
Automated Scanning/Attacking Doesn't Care Who You Are 431
Desirable Resources Make You a Target 431
Political or Emotional Motivations 432
Where Does an IDS Fit with the Rest of My Security Plan? 433
Where Should I Be Looking for Intrusions? 433

Operating System Security—Backdoors and Trojans 434
Physical Security 434
Application Security and Data Integrity 436
Correlation of All These Sources 437
What Will an IDS Do for Me? 437
Continuously Watch Packets on Your Network and Understand Them 437
Read Hundreds of Megs of Logs Daily and Look for Specific Issues 438
Create Tremendous Amounts of Data No Matter How Well You Tune It 438
Create So Much Data that If You Don't Tune It, You Might as Well Not Have It 439
Find Subtle Trends in Large Amounts of Data that Might Not Otherwise Be Noticed . . .439
Supplement Your Other Protection Mechanisms . .439
Act as a Force Multiplier Competent System/ Network Administrator 440
Let You Know When It Looks Like You Are Under Attack 440
What Won't an IDS Do for Me? 441
Replace the Need for Someone Who Is Knowledgeable about Security 441
Catch Every Attack that Occurs 441
Prevent Attacks from Occurring 442
Prevent Attacks from Succeeding Automatically (in Most Cases) 443
Replace Your Other Protection Mechanisms 444
What Else Can Be Done with Intrusion Detection? . .444
Fitting Snort into Your Security Architecture 444
Viruses, Worms, and Snort 445
Known Exploit Tools and Snort 445
Writing Your Own Signatures with Snort 446
Using an IDS to Monitor Your Company Policy 446
Analyzing Your IDS Design and Investment 446
False Positives versus False Negatives 447

Fooling an IDS .447
IDS Evasion Techniques .447
Return on Investment—Is It Worth It? .449
Defining IDS Terminology .450
Intrusion Prevention Systems (HIPS and NIPS) .450
Gateway IDS .450
Network Node IDS .450
Protocol Analysis .451
Target-Based IDS .451
Summary .452
Solutions Fast Track .452
Frequently Asked Questions .454
Appendix C Introducing Vulnerability Assessments and Nessus .455
Introduction .456
What Is a Vulnerability Assessment? .456
Why a Vulnerability Assessment? .458
Assessment Types .459
Host Assessments .460
Network Assessments .461
Automated Assessments .461
Stand-Alone vs. Subscription .462
The Assessment Process .463
Detecting Live Systems .463
Identifying Live Systems .464
Enumerating Services .464
Identifying Services .466
Identifying Applications .466
Identifying Vulnerabilities .467
Reporting Vulnerabilities .468
Two Approaches .469
Administrative Approach .469
The Outsider Approach .470
The Hybrid Approach .471
Realistic Expectations .473
The Limitations of Automation .475

Summary 476
Solutions Fast Track 477
Frequently Asked Questions 478

Index 481

About the CD

The CD-ROM accompanying this book contains the Windows to Linux Migration Toolkit (W2LMT) scripts and configuration files, as well as a chapter-by-chapter summary of the configuration files used by the fictional companies Acme Widgets and Ballystyx Engineering. Navigate to **index.html** for an easy-to-use chapter-by-chapter guide to the features of the CD

The following table lists each directory, chapter affiliation, and a description of the files located in that directory. It is important to note that although the package directory listed below does contain the latest versions of the Open Source tools used in the book at the time of publication, most Open Source projects develop and evolve at a rapid pace; the scripts may be updated or outmoded by the time you read this. You may want to obtain the latest versions from the appropriate websites, including the W2L MT (Windows to Linux Migration Toolkit), found at www.syngress.com/solutions and http://souceforge.net/projects/w2lmt.

Directory	Chapter	Contents
Chap01	Network Migration Roadmap	-
Chap02	Core TCP/IP Services	DHCP/DNS and migration script configuration files
Chap03	Directory Services	OpenLDAP configuration files
Chap04	Authentication Services	Samba and directory/auth migration script configuration files

Continued

Directory	Chapter	Contents
Chap05	File Services	-
Chap06	Print Services	-
Chap07	Messaging Services	Mailbox migration script configuration files
Chap08 (Outport)	Groupware and Calendaring	Outlook Export tool
Chap09	Web Services	-
Chap10	Desktop Migration Roadmap	-
Chap11	Inside the Linux Desktop	-
Etc	ALL	Generic configuration files for w2lmt with comments
Package	ALL	Packaged binaries and compressed source files of many of the tools mentioned in the book, including w2lmt, and all the dependencies required to install them
Src	ALL	W2lmt scripts in source form
et_sn_ns	Appendix A	Ethereal
et_sn_ns	Appendix B	Snort
et_sn_ns	Appendix C	Nessus