

SANS GIAC

CERTIFICATION:

Security Essentials Toolkit (GSEC)

Eric Cole
Mathew Newfield
John M. Millican



201 West 103rd Street, Indianapolis, Indiana 46290

SANS GIAC CERTIFICATION: SECURITY ESSENTIALS TOOLKIT (GSEC)

Copyright © 2002 by Que Publishing

All rights reserved. No part of this book shall be reproduced, stored in a retrieval system, or transmitted by any means, electronic, mechanical, photocopying, recording, or otherwise, without written permission from the publisher. No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

International Standard Book Number: 0-7897-2774-9

Library of Congress Catalog Card Number: 2002101824

Printed in the United States of America

First Printing: March 2002

04 03 02 4 3 2 1

Trademarks

All terms mentioned in this book that are known to be trademarks or service marks have been appropriately capitalized. Que Publishing cannot attest to the accuracy of this information. Use of a term in this book should not be regarded as affecting the validity of any trademark or service mark.

Warning and Disclaimer

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an “as is” basis. The authors and the publisher shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book.

PUBLISHER

David Culverwell

SENIOR ACQUISITIONS EDITOR

Jeff Riley

DEVELOPMENT EDITOR

Ginny Bess Munroe

MANAGING EDITOR

Thomas F. Hayes

PROJECT EDITOR

Thomas F. Hayes

COPY EDITOR

Ginny Bess Munroe

INDEXER

Tom Dinse

PROOFREADER

Megan Wade

TECHNICAL EDITORS

Mike Poor

David Goldsmith

Sheila Ettinger

INTERIOR DESIGNER

Anne Jones

COVER DESIGNER

Aren Howell

CONTENTS AT A GLANCE

Introduction

1 Security Overview

PART I SECURITY OVERVIEW

2 Trojans

3 Host-Based Intrusion Detection

4 Network-Based Intrusion Detection

5 Firewalls

6 Scanning Tools

PART II SECURITY CONCEPTS

7 Understanding Exploits

8 Security Policy

9 Password Cracking

10 Forensic Backups

11 Denial of Service and Deception Attacks

12 Web Security

PART III NETWORK SECURITY

13 Network Design

14 Base Conversions, IP Addressing, and Subnetting

15 Network Security Tools

PART IV SECURE COMMUNICATIONS

16 Secure Communications

PART V WINDOWS

17 Windows Security

PART VI UNIX

18 Unix

19 Summary

Index

TABLE OF CONTENTS

Introduction	1	Exercise 3: Trojan Software SubSeven	49
Who Should Read This Book	1	Description	49
What's in This Book	2	Objective	49
Conventions Used in This Book	2	Requirements	49
1 Security Overview	5	Challenge Procedure	49
Introduction to Security Tools	5	Challenge Procedure Step-by-Step	49
Exercise 1: Configuring Your System	9	Additional Reading	53
Description	9	Summary	53
Requirements	9	3 Host-Based Intrusion Detection	55
Challenge Procedure	10	Exercise 1: TCP Wrappers	55
Challenge Procedure Step-by-Step	10	Description	55
Additional Reading	29	Objective	56
Summary	29	Requirements	56
Acronyms List	29	Challenge Procedure	56
PART I SECURITY OVERVIEW		Challenge Procedure Step-by-Step	56
2 Trojans	41	Additional Reading	59
Exercise 1: Trust Relationships	41	Summary	59
Description	41	Exercise 2: xinetd	60
Objective	42	Description	60
Requirements	42	Objective	60
Challenge Procedure	42	Requirements	60
Challenge Procedure Step-by-Step	43	Challenge Procedure	60
Additional Reading	44	Challenge Procedure Step-by-Step	61
Summary	44	Additional Reading	65
Exercise 2: Trojan Software NetBus	45	Summary	65
Description	45	Exercise 3: Tripwire	66
Objective	45	Description	66
Requirements	45	Objective	66
Challenge Procedure	45	Requirements	66
Challenge Procedure Step-by-Step	45	Challenge Procedure	66
Additional Reading	48	Challenge Procedure Step-by-Step	67
Summary	48	Additional Reading	73
		Summary	73
		Exercise 4: Swatch	74
		Description	74
		Objective	74
		Requirements	74
		Challenge Procedure	74
		Challenge Procedure Step-by-Step	74

Additional Reading	78	Challenge Procedure	99
Summary	78	Challenge Procedure Step-by-Step	99
Exercise 5: PortSentry	79	Additional Reading	103
Description	79	Summary	103
Objective	79		
Requirements	79	5 Firewalls	105
Challenge Procedure	79	Exercise 1: Personal Firewalls and ZoneAlarm	105
Challenge Procedure Step-by-Step	79	Description	105
Additional Reading	82	Objective	105
Summary	82	Requirements	105
Exercise 6: Auditing Your System	83	Challenge Procedure	105
Description	83	Challenge Procedure Step-by-Step	105
Objective	83	Additional Reading	109
Requirements	83	Summary	109
Challenge Procedure	83	Exercise 2: Tiny Firewall	110
Challenge Procedure Step-by-Step	83	Description	110
Additional Reading	88	Objective	110
Summary	88	Requirements	110
4 Network-Based Intrusion Detection	89	Challenge Procedure	110
Exercise 1: Sniffing with tcpdump	89	Challenge Procedure Step-by-Step	110
Description	89	Additional Reading	116
Objective	89	Summary	116
Requirements	89	Exercise 3: ipchains	117
Challenge Procedure	90	Description	117
Challenge Procedure Step-by-Step	90	Objective	118
Additional Reading	93	Requirements	118
Summary	93	Challenge Procedure	118
Exercise 2: Nuking a System	94	Challenge Procedure Step-by-Step	118
Description	94	Additional Reading	124
Objective	94	Summary	124
Requirements	94	6 Scanning Tools	125
Challenge Procedure	94	Exercise 1: Scanning with Nmap	125
Challenge Procedure Step-by-Step	94	Description	125
Additional Reading	98	Objective	125
Summary	98	Requirements	125
Exercise 3: Snort	99	Challenge Procedure	126
Description	99	Challenge Procedure Step-by-Step	126
Objective	99	Additional Reading	130
Requirements	99	Summary	130

Exercise 2: Scanning with SuperScan	131	Challenge Procedure Step-by-Step	154
Description	131	Additional Reading	155
Objective	131	Summary	155
Requirements	131		
Challenge Procedure	131	Exercise 2: Extracting Information with	
Challenge Procedure Step-by-Step	132	DumpSec	156
Summary	135	Description	156
		Objective	156
Exercise 3: Vulnerability Scanning with		Requirements	156
Nessus	136	Challenge Procedure	156
Description	136	Challenge Procedure Step-by-Step	156
Objective	136	Additional Reading	159
Requirements	136	Summary	159
Challenge Procedure	136		
Challenge Procedure Step-by-Step	136	8 Security Policy	161
Additional Reading	140	Exercise 1: Developing a Security Policy	161
Summary	140	Description	161
		Objective	161
Exercise 4: Legion	141	Requirements	161
Description	141	Challenge Procedure	161
Objective	141	Challenge Procedure Step-by-Step	161
Requirements	141	Additional Reading	165
Challenge Procedure	141	Summary	165
Challenge Procedure Step-by-Step	141		
Summary	144	9 Password Cracking	167
		Exercise 1: John the Ripper	167
Exercise 5: hping2	145	Description	167
Description	145	Objective	167
Objective	145	Requirements	167
Requirements	145	Challenge Procedure	168
Challenge Procedure	145	Challenge Procedure Step-by-Step	168
Challenge Procedure Step-by-Step	145	Additional Reading	170
Additional Reading	148	Summary	170
Summary	149		
		Exercise 2: L0pht Crack (LC3)	171
PART II SECURITY CONCEPTS		Description	171
7 Understanding Exploits	153	Objective	171
Exercise 1: Null Session Exploits	153	Requirements	171
Description	153	Challenge Procedure	171
Objective	153	Challenge Procedure Step-by-Step	171
Requirements	154	Additional Reading	176
Challenge Procedure	154	Summary	176

10 Forensic Backups	177	<i>Challenge Procedure</i>	200
Exercise 1: Disk Imaging with Ghost	177	<i>Challenge Procedure Step-by-Step</i>	200
Description	177	<i>Additional Reading</i>	202
Objective	177	<i>Summary</i>	202
Requirements	177	Exercise 2: Web Security with WebSleuth	203
Challenge Procedure	177	Description	203
Challenge Procedure Step-by-Step	178	Objective	203
Additional Reading	186	Requirements	203
Summary	186	Challenge Procedure	203
Exercise 2: Forensics with dd	187	Challenge Procedure Step-by-Step	204
Description	187	Additional Reading	208
Objective	187	Summary	208
Requirements	187	Exercise 3: Finding Web Vulnerabilities	
Challenge Procedure	187	with Whisker	209
Challenge Procedure Step-by-Step	187	Description	209
Additional Reading	189	Objective	209
Summary	190	Requirements	209
11 Denial of Service and Deception Attacks	191	Challenge Procedure	210
Exercise 1: Denial of Service with TFN2K	191	Challenge Procedure Step-by-Step	210
Description	191	Additional Reading	214
Objective	191	Summary	214
Requirements	191	PART III NETWORK SECURITY	
Challenge Procedure	192	13 Network Design	217
Challenge Procedure Step-by-Step	192	Exercise 1: Cisco ConfigMaker	217
Summary	194	Description	217
Exercise 2: Deception with Fragrouter	195	Objective	217
Description	195	Requirements	217
Objective	195	Challenge Procedure	217
Requirements	195	Challenge Procedure Step-by-Step	218
Challenge Procedure	195	Additional Reading	235
Challenge Procedure Step-by-Step	195	Summary	235
Summary	198	14 Base Conversions, IP Addressing, and	
12 Web Security	199	Subnetting	237
Exercise 1: Web Security with BlackWidow	199	Exercise 1: Binary Conversion	237
Description	199	Description	237
Objective	199	Objective	237
Requirements	199	Requirements	237

Challenge Questions	237
Challenge Procedure Step-by-Step	237
Challenge Solution	238
Additional Reading	238
Summary	238
Exercise 2: Subnetting	239
Description	239
Objective	239
Requirements	239
Challenge Procedure	240
Challenge Procedure Step-by-Step	240
Additional Reading	244
Summary	244
15 Network Security Tools	245
Exercise 1: Router ACLs	245
Description	245
Objective	245
Requirements	245
Challenge Procedure	245
Challenge Procedure Step-by-Step	246
Additional Reading	248
Summary	248
Exercise 2: Scanning Hosts with Ping War	249
Description	249
Objective	249
Requirements	249
Challenge Procedure	249
Challenge Procedure Step-by-Step	249
Additional Reading	252
Summary	252
Exercise 3: Analysis with Ethereal	253
Description	253
Objective	254
Requirements	254
Challenge Procedure	254
Challenge Procedure Step-by-Step	254
Summary	269

PART IV SECURE COMMUNICATIONS

16 Secure Communications	273
Exercise 1: PGP	273
Description	273
Objective	273
Requirements	273
Challenge Procedure	274
Challenge Procedure Step-by-Step	274
Additional Reading	277
Summary	277
Exercise 2: Steganography with JPHS	278
Description	278
Objective	278
Requirements	278
Challenge Procedure	278
Challenge Procedure Step-by-Step	278
Summary	284
Exercise 3: Steganography with S-Tools	285
Description	285
Objective	285
Requirements	285
Challenge Procedure	285
Challenge Procedure Step-by-Step	285
Additional Reading	288
Summary	288

PART V WINDOWS

17 Windows Security	291
Exercise 1: Security Configuration and Analysis	291
Description	291
Objective	291
Requirements	291
Challenge Procedure	291
Challenge Procedure Step-by-Step	292
Additional Reading	296
Summary	296

Exercise 2: Startup Cop	297
Description	297
Objective	297
Requirements	297
Challenge Procedure	297
Challenge Procedure Step-by-Step	297
Summary	299
Exercise 3: Hfnetchk	300
Description	300
Objective	300
Requirements	300
Challenge Procedure	300
Challenge Procedure Step-by-Step	300
Additional Reading	304
Summary	304
Exercise 4: MPSA	305
Description	305
Objective	305
Requirements	305
Challenge Procedure	305
Challenge Procedure Step-by-Step	305
Summary	307
Exercise 5: How to Baseline and Audit Your System	308
Description	308
Objective	308
Requirements	308
Challenge Procedure	308
Challenge Procedure Step-by-Step	308
Additional Reading	314
Summary	314
Exercise 6: Backups	315
Description	315
Objective	315
Requirements	315
Challenge Procedure	315
Challenge Procedure Step-by-Step	315
Additional Reading	320
Summary	321

Exercise 7: IIS Lockdown	322
Description	322
Objective	322
Requirements	322
Challenge Procedure	322
Challenge Procedure Step-by-Step	322
Additional Reading	325
Summary	325
Exercise 8: Socket80	326
Description	326
Objective	326
Requirements	326
Challenge Procedure	326
Challenge Procedure Step-by-Step	326
Additional Reading	329
Summary	329

PART VI UNIX

18 Unix	333
Exercise 1: The Unix File System	333
Description	333
Objective	333
Requirements	333
Challenge Procedure	333
Challenge Procedure Step-by-Step	333
Additional Reading	338
Summary	338
Exercise 2: Sudo	339
Description	339
Objective	339
Requirements	339
Challenge Procedure	339
Challenge Procedure Step-by-Step	339
Additional Reading	342
Summary	342
Exercise 3: Unix Permissions	343
Description	343
Objective	343
Requirements	343
Challenge Procedure	343

<i>Challenge Procedure Step-by-Step</i>	343
<i>Additional Reading</i>	345
<i>Summary</i>	345
Exercise 4: Unix Network Commands	346
<i>Description</i>	346
<i>Objective</i>	346
<i>Requirements</i>	346
<i>Challenge Procedure</i>	346
<i>Challenge Procedure Step-by-Step</i>	346
<i>Additional Reading</i>	347
<i>Summary</i>	347
Exercise 5: Log Files	348
<i>Description</i>	348
<i>Objective</i>	348
<i>Requirements</i>	348
<i>Challenge Procedure</i>	348
<i>Challenge Procedure Step-by-Step</i>	348
<i>Additional Reading</i>	350
<i>Summary</i>	350

Exercise 6: tar	351
<i>Description</i>	351
<i>Objective</i>	351
<i>Requirements</i>	351
<i>Challenge Procedure</i>	351
<i>Challenge Procedure Step-by-Step</i>	351
<i>Additional Reading</i>	352
<i>Summary</i>	352
19 Summary	353
Index	355

FOREWORD

More people have taken the SANS Security Essentials course than any other information security course in the world, and the numbers are growing rapidly. Today, our job in security is so complex that each of us must realize we have significant gaps in our understanding. Security Essentials fills the gaps. A few people have played notable roles in developing the courseware, though it is the product of several hundred security practitioners in the defensive community working together, and it continues to evolve to meet the needs of the students.

Security Essentials was born at the SANS 1999 annual conference in Baltimore, Maryland. Alan Paller, Director of Research for SANS, had been trying to develop a program to cover only those elements you need to know about information security and nothing else; however, it had been slow and painful. Everyone who worked on the project ended up giving up after a couple of weeks. I was very busy at the time, but Alan would tell me what he had attempted and why it didn't work. I would nod and express my condolences being careful not to volunteer my opinions or help. I wanted to help, but it sounded like a tremendous amount of effort involving potentially thousands of hours. However, I too was frustrated. I was a manager for the Department of Defense, and it was hard to hire people with the skills to do the jobs we needed done. At best, potential employees understood the theory of security, and they understood that those theories tended to originate from a mainframe era. I thought if I could just hire people who met a minimum standard, my life would be ten times easier. Prior to departing for Baltimore, I knew that for better or worse, I was going to take the lead for the Security Essentials project. It was too important a project, and I wanted to help Alan get it off the ground.

On the third day of the conference, I had a day off, one of the few days when I wasn't teaching, so Alan and I got in a harbor taxi boat to get away from the noise and excitement of the conference. We had a set of index cards with us, and as soon as we go on the boat, we started brainstorming on those cards. We

knew we had to figure out what people needed to know, or what was critical versus what wasn't critical. We asked ourselves, "What are the essentials of information security for the practitioner?"

When we got back to the conference speaker room, Fred Kerby, an information security manager for the U.S. Navy, took the cards and started to create a list from what we had written. Michele Guel, Hal Pomeranz, and other instructors debated the list and added their unique perspectives. Dr. Eugene Schultz, founder of CIAC and an instructor, contributed to an hour-long conference call expressing his concerns and giving us his suggestions. We arrived at version .21 of the course. The fact that we were not yet at a full-numbered version tells you how far we felt we needed to go. We then had objectives and domains of knowledge reviewed by the CIO Institute to get feedback from senior management and from as many system, network, and security administrators in the trenches as we could find.

Finally, we began development of the first course modules by starting with what we thought were the absolutely necessary courses, such as cryptography, malicious code, how IP works, and threat and risk assessment. At the time, we were hoping to partner with ISC2, the company that produces the CISSP. We shared the design, objectives, and courseware developed at the time, and we asked for guidance on what they thought might be missing, or what needed to be covered differently. Eventually, after 99 revisions, we reached version 1.0 of Security Essentials. Before anyone outside of the development team ever saw the courseware, over a hundred security experts from 15 different countries had invested in the creation of Security Essentials.

The goal of this project from the beginning was for it to represent a consensus of the global community. Special thanks should be offered to Philip Boyle, an IT worker from New Zealand; Guy Bruneau who worked in the DnD Cirt from Canada; Andrew Sturman, a consultant from the United Kingdom; and Dean White, an intrusion detection analyst from Australia. We also felt that the only way to distribute this product globally was to offer

an online version of the course. Jennifer Kolde, Director of the GIAC Certification, was instrumental in formatting the early courseware. Dave Turley, a lead programmer for SANS, wrote the software delivery system for both the courses and exams, which he built on the work that Rob Kolstad started. John Green, the second leader of the “Shadow team” and co-founder of Incidents.org, created the powerful database that tracks registration and accounting for both the live and online training. Doug Austin, a consultant, developed the system we use for digital audio. Karen Ellrick, a musician and missionary in Japan, helped us make a huge breakthrough when she suggested we convert from audio tapes as our sound source to mini-disks. The higher-quality source material resulted in better sounding files, one of the biggest problems we had to overcome and did, thanks to Karen.

Eric Cole, the lead author of this workbook, was involved with the project since the early days, and he is a top-notch instructor of the courseware. When we realized that we were going to have to expand the program from three to six days to cover the material properly, Eric took the lead role in the conversion.

The course is being taught somewhere in the world almost weekly, in conferences, in private onsite sessions, or in the form of a local, mentoring project. We’ve seen the course taught just about everywhere, from Atlanta, Georgia, to Honolulu, Hawaii to Dubai.

I am thankful to have had the best seat in the house from which I could watch this course grow. I have met a lot of wonderful people, and I know that together we are making a difference. I thank God for giving me the courage to work on this project. It is by far the most challenging project I have ever worked on. I missed out on a lot of sleep and many swims off the beaches of Kauai with my wife and son, but I feel it was, and is, worth the sacrifice. The day is coming when it will be impossible to be considered a credible information security practitioner without holding a GIAC Security Essentials Certification.

This book is a very positive step forward in the evolution of the program. I want to thank Eric Cole, Matt Newfield, John Millican, and the review team for their tremendous efforts. It takes tools to get work done, and this workbook will help practitioners acquire and use the tools that will help accomplish the essential work of security. Take your time, master the tools, and take notes (there is space to do this in the book) while building a toolbox that works for you. We care deeply about your experiences, what works for you, and what doesn’t work for you. We want to know the things you know or don’t know, so don’t be a stranger.

Stephen Northcutt

The SANS Institute

ABOUT THE AUTHORS

Eric Cole has worked in the information security arena for more than 10 years. He holds several professional certifications and has helped develop several of the SANS GIAC certifications and corresponding courses. Eric has a BS and MS in computer science from New York Institute of Technology and is completing his Ph.D. in network security. He has extensive experience with all aspects of information security including the following: cryptography, stenography, intrusion detection, NT security, Unix security, TCP/IP and network security, Internet security, router security, security assessment, penetration testing, firewalls, secure Web transactions, electronic commerce, SSL, TLS, IPSec, and information warfare.

Eric has created and headed up corporate security for several large organizations, built several security consulting practices, and worked for more than five years at the Central Intelligence Agency. He was an adjunct professor at New York Institute of Technology and is currently an adjunct professor at Georgetown University. Eric is author of the book *Hackers Beware* and contributing author to *Know Thy Enemy: The HoneyNet Project*. Eric teaches a wide range of courses for SANS and is actively involved with several of the research projects that SANS is performing. He led the SANS Top 20 vulnerability consensus project and is actively involved with the Cyber Defense Initiative.

Mathew Newfield serves as a Senior Security Analyst for TruSecure Corporation. His background includes penetration testing, security architecture, and design and network consulting. He currently works with several companies in securing their environments and obtaining corporate security certifications.

John M. Millican has been providing information consulting services since 1978. During that time, he has supported numerous versions of Unix, including AT&T, CTIX, SCO Unix, AIX, Unixware, and Linux. John was the first person to earn all the GIAC Level 2 Certifications offered by the SANS Institute. He is certified by SANS GIAC for Intrusion Detection In Depth (GCIA); Advanced Incident Handling and Hacking Exploits (GCIH); Firewalls, VPNs, and Perimeter Protection (GCFW); Securing Windows (GCFW); Securing Unix (GCUX); and Auditing Networks, Perimeters, and Systems (GCNA). He is currently the chairman of the SANS Unix Security Certification Board. John also assisted in the development of the SANS Security Essentials Bootcamp.

TECHNICAL REVIEWERS

Mike Poor is a security analyst for Compugenx, a Washington, D.C.-based consulting company. He holds SANS, GSEC, and GCIA certifications. As a security analyst, he conducts vulnerability assessments, penetration tests and security audits and administers intrusion detection systems. Previously, Mike has worked in network engineering and systems, network, and Web administration. He is currently working on merging Snort, Shadow, and ngrep to bring more analytical power to the analyst.

Sheila Ettinger is gainfully employed as a Unix Systems Administrator at Concordia University in Montreal. In her previous life, she worked in contract research and as a technical writer, software tester, and Windows trainer. Sheila is currently part of the design team involved in a project to reorganize Concordia's IT services. (She is being dragged kicking and screaming into the world of Active Directory. We'll let you know if she survives.)

In addition to her day job, Sheila teaches evening computer courses at Concordia's Center for Continuing Education and is a Program Consultant for the center's Computer Institute. In her down time, she enjoys playing clarinet in a number of community concert bands and taking courses in the university's music department.

David Goldsmith has been working in the computer and network industry for over 10 years, of which he has focused the last 3 on Internet connectivity and system/network security. From 1990 to 1995, he worked for the USMC as a system/network administrator and systems engineer. From 1995 to 1999, he worked for Ocean Systems Engineering Corporation providing system administration and network security support for the USMC. David currently has his own business, Rappahannock Technologies, Incorporated, which focuses on providing network security consulting services to commercial companies. He holds a degree in computer science from the University of California, San Diego.

DEDICATION

From Eric Cole:

To my loving wife for all her support.

From Mathew Newfield:

I would like to dedicate this book to my son Samuel.

From John M. Millican:

I dedicate this to my wife for all of her support throughout our years together.

ACKNOWLEDGMENTS

From Eric Cole:

I want to thank Que Certification for their help and support through this process, mainly Jeff Riley and Ginny Bess. They are a great publishing team to work with and have proven that the only way to produce a great product is to have fun doing it.

I also want to thank SANS for being such a great organization. Alan Paller and Stephen Northcutt are wonderful people to work with and very helpful. They gave me great advice and support throughout the process of writing this book.

What always makes me nervous about including an acknowledgments section is the thought that I might overlook someone. When this book comes out, I am going to remember who I forgot. Thus, I am dedicating a blank line here for those I forgot to acknowledge. You can write your name into this section _____.

Most of all, I want to thank God for blessing me with a great life and a wonderful family. Kerry Magee Cole is a loving and supportive wife. My wonderful son, Jackson, brings me joy and happiness every day. I'm also grateful for the new special blessing in our life who will be arriving in June. Ron and Caroline Cole and Mike and Ronnie Magee are

great parents to me and offer both love and support. Finally, I'm grateful for a wonderful sister, brother-in-law, nieces, and nephews: Cathy, Tim, Allison, Timmy, and Brianna.

For anyone who I forgot or did not mention by name, I thank you, especially my friends, family, and co-workers, who have supported me in numerous ways throughout this entire process.

From Mathew Newfield:

I would like to thank my wife Jennifer, my son Samuel, my mother and Bill, my father and Sarah, and all of my friends for always being there for me. I would also like to thank TruSecure Corporation and especially Bill Harrod and Kristen Lovejoy for giving me the support, time, and opportunity to dedicate to this project.

From John M. Millican:

I would like to thank my wife Jill, my daughter Julie, and my son Chris for their support and patience during this long, strange trip. I would also like to add my expression of appreciation to the entire SANS community. It is their commitment to helping develop the information security community that has offered these opportunities to me.

TELL US WHAT YOU THINK!

As the reader of this book, *you* are our most important critic and commentator. We value your opinion and want to know what we're doing right, what we could do better, what areas you'd like to see us publish in, and any other words of wisdom you're willing to pass our way.

As a senior acquisitions editor for Que Certification, I welcome your comments. You can fax, email, or write me directly to let me know what you did or didn't like about this book—as well as what we can do to make our books stronger.

Please note that I cannot help you with technical problems related to the topic of this book, and that due to the high volume of mail I receive, I might not be able to reply to every message.

When you write, please be sure to include this book's title and authors as well as your name and phone. I will carefully review your comments and share them with the authors and editors who worked on the book.

Fax: 317-581-4666
Email: jeff.riley@quepublishing.com
Mail: Que
201 West 103rd Street
Indianapolis, IN 46290 USA

Introduction

The SANS (System Administration, Networking, and Security) Institute is a cooperative research and education organization through which more than 96,000 system administrators, security professionals, and network administrators share the lessons they are learning and find solutions to the challenges they face. SANS was founded in 1989.

The core of the institute consists of security practitioners in government agencies, corporations, and universities around the world who invest hundreds of hours each year in research and teaching to help the entire SANS community. During 2000 and 2001, this core group grew rapidly as the Global Information Assurance Certification program developed mentors to help new security practitioners master the basics.

The SANS community creates four types of products:

- System and security alerts and news updates
- Special research projects and publications
- In-depth education
- Certification

Several SANS resources, such as news digests, research summaries, security alerts, and award-winning papers, are free. Income from printed publications funds university-based research programs. The Global Information Assurance Certification program and special research projects are funded by income from SANS educational programs.

SANS's GIAC (Global Information Assurance Certification) is one of the fastest growing areas among the institute's educational offerings. GIAC online training caters to the needs of security professionals, from those who are just getting started with the Information Security KickStart module, to the advanced GIAC Security Engineer honors program. Over 1,000 students have achieved GIAC certification, and many more are currently in the process of achieving it.

For more information, see <http://www.sans.org> or <http://www.giac.org>.

WHO SHOULD READ THIS BOOK

This book is beneficial to those who are interested in security or those who are new to security. It covers the essential tools and concepts that you need to understand in order to be a productive security professional. If you have been working in the security field, you will still find value in the material presented in this book. You might be familiar with some of the tools, but several of the tools will be new to you, or you might discover new ways of using a tool. In summary, this book is meant to provide a hands-on style of learning that compliments the SANS Security Essentials course. This book was written to provide value as an independent text. We wrote this book under the general principle that if we could teach you about the tools, you would be prepared to conquer any security task.

NOTES

WHAT'S IN THIS BOOK

This book is about the tools. There is so much work to be done in security. Manual methods are just too time-consuming. If we use the most valuable tools, and we understand the benefits of them, we will be more productive with our time. With this premise in mind, this book covers tools across all areas of security, as noted in this list:

- Security Overview
- Security Concepts
- Network Security
- Secure Communications
- Windows Security
- Unix Security

Each section of the book is broken up into chapters that cover a number of tools.

CONVENTIONS USED IN THIS BOOK

Each chapter is composed of a set of exercises, each of which features a specific tool. The idea is for you to learn how to install and use the tools so that you can apply your knowledge to secure your company's network and computer systems. To make the tools and exercises easy to understand, the following format is used to describe each exercise:

- **Description** The Description section provides an overview of the tool being discussed in the exercise and where it fits in the overall security scheme. Background information and other relevant data are also described in this section.
- **Objective** Every tool is designed for a specific purpose or domain of use. The Objective section describes the purpose of the tool and what skills you should gain by completing the exercise and running the tool.
- **Requirements** Whatever is required in order to run the exercise and utilize the tool is described in this section.

Subsections of the Requirements section include the following:

Permission Keep in mind that some of the tools discussed can compromise systems or perform actions that could be deemed illegal in some countries or states. Thus, this section explains when you need to gain permissions.

Hardware Various programs require hardware or components to run. Hardware requirements are listed in this section.

Software Various programs run on different operating systems and require other programs to be loaded. Software that is needed in order to run a tool or complete an exercise is listed in this section.

- **Challenge Procedure** The Challenge Procedure sections provide an overview of the steps that you perform to complete the exercises.
- **Challenge Procedure Step-by-Step** This section provides a detailed step-by-step instruction of the steps required to install, configure, and run the tool that is discussed in the Description section and Challenge Procedure section. Screen shots are provided to make this section as straightforward and easy as possible to follow.
- **Challenge Questions** Throughout the step-by-step procedures, questions are periodically inserted that challenge you to think about other ways the tools can be used to help expand your knowledge and understanding of the concepts that are being described.
- **Additional Reading** Additional reference materials are recommended for several of the exercises. These include articles, papers, or books. They are listed in this section.
- **Summary** The Summary section ties together what you have learned in each section. The summaries also serve to summarize the bigger picture helping you to resolve the puzzles of network security. Any other features or functions of the system are also described in this section.

- **Commands, Screen Captures, Menus, Keys, and Buttons**

For your convenience, we highlighted in bold commands and items that are “selected” or “clicked.” We also highlighted in bold the names of screens, menus, keys, and buttons. We used this convention to make your work easier and to make the exercises easier to follow.

- **Notes** Periodically, we inserted notes to supplement your understanding of specific topics. In addition, we provided you space to take your own notes. Use this space to jot down tips or instructions that you want to take back to your organization. Or, use it to jot down questions you might want to pursue when you research some of the “Additional Reading” references.

Remember, the best way to learn is to experiment and test each of these tools. Download them, install and run them on your system, and learn the value they can offer your security strategies. Above all else, have fun as you take steps toward securing your organization.

NOTES

NOTES



Security Overview

INTRODUCTION TO SECURITY TOOLS

Security is a complex field. Manually testing and securing your systems can be a daunting task at best and impossible at worst. Thankfully, there are numerous tools available that can help secure your site with minimal effort. With these tools, you will still have to analyze the results, but at least a bulk of the work is done for you.

The purpose of this book is to provide you with the exact steps for installing, configuring, and running the most popular security software tools on your systems. To teach you in the most efficient manner, we've developed a workbook-style approach. This book also concentrates on shareware and freeware tools emphasizing the fact that you do not need to spend a lot of money in order to have a secure network.

The following table shows you the tools that will be discussed in this book.

NOTES

Shareware and Freeware Security Tools

Application	Description	Available At
BlackWidow	An offline Web site browser and information tool	http://www.softbytelabs.com/files/BlackWidow.exe
Cisco ConfigMaker v2.5.1	Cisco network configuration tool	http://www.cisco.com/univercd/cc/td/doc/clickstrt/cfgmkr/download.htm
Crack	A password cracker	http://www.users.dircon.co.uk/~crypto/download/c50-faq.html
Dumpel	Dumps the contents of the Windows NT and Windows 2000 event logs	http://www.microsoft.com/windows2000/techinfo/reskit/tools/existing/dumpel-o.asp
DumpSec	Windows security auditing program	http://www.somarsoft.com/somarsoft_main.htm
Ethereal	Network sniffing and packet analysis tool	http://www.ethereal.com/distribution/win32/ethereal-setup-0.9.0-1.exe
Forensic Toolkit	File properties analyzer	http://www.foundstone.com/rdlabs/tools.php?category=Forensic
Fport	Reports all open TCP and UDP ports and maps them to the running application	http://www.foundstone.com/rdlabs/termsofuse.php?filename=FportNG.zip
Fragrouter	A tool to fragment packets sent from a host to a target	http://www.packetstormsecurity.com
Ghost Corporate Edition	DOS-based disk cloning	http://www.enterprisesecurity.symantec.com/content/productlink.cfm?
HFNETCHK	A tool developed by Microsoft to help administrators stay current with system patches	http://www.microsoft.com/downloads/release.asp?releaseid=31154
Hping2	An advanced tool that expands on ICMP functionality	http://www.hping.org/hping2.0.0-rc1.tar.gz
IIS Lockdown	A tool to assist in the hardening of an IIS installation	http://www.microsoft.com/Downloads/Release.asp?ReleaseID=32362
John the Ripper	A password cracker	http://www.packetstormsecurity.com
Jphs	A Windows-based steganography tool	http://www.linux01.gwdg.de/~alatham/stego.html
Jsteg	A Windows-based steganography tool	http://www.tiac.net/users/korejwa/jsteg.htm
LeakTest	Tests personal firewalls to determine if they warn when outbound connections are made	http://www.grc.com/lt/leaktest.htm
Legion	A Windows-based share scanner	http://www.nmrc.org/files/snt
Logcheck v1.1.1	Unix log monitoring system	http://www.psionic.com/abacus/logcheck
L0pht Crack 3.0	A password cracker	http://www.atstake.com/research/lc3/
Nessus	A Linux-based vulnerability scanner	http://www.nessus.org

Shareware and Freeware Security Tools Continued

Application	Description	Available At
Netbus 1.7	Remote control trojan software	http://www.packetstorm.decepticons.org/trojans/NetBus170.zip
nmap	A Linux-based port scanning utility	http://www.insecure.org/nmap/nmap_download.html
pgp	Encryption software for files and email	http://www.pgpi.org/products/pgp/versions/freeware/
Ping War	A Windows-based tool to quickly ping a large range of IP addresses	http://www.simtel.net/autodownload.html?mirror=5&product=17874&key=00dbb38ca3570c3050b1
Psionic PortSentry 1.1	Unix port monitoring tool	http://www.psionic.com/tools/portsentry-1.1.tar.gz
Purge-It!	Trojan removal helper application	http://www.purge-it.com
PWDump3	A password cracker	http://www.ebiz-tech.com/pwdump3
S-tools	A Windows-based steganography tool	http://www.members.tripod.com/steganography/stego/software.html
Snort	A freeware IDS and packet sniffer	http://www.snort.org/downloads.html#1.19
Socket 80	A GUI-based application that runs Unicode attacks against IIS servers	http://www.astalavista.com/tools/auditing/network/http-server/
Startup Cop	A tool to create startup profiles in Windows	http://www.pcmag.com/article/0,2997,s=400&a=8066,00.asp?download_url=http://common.ziffdavisinternet.com/download/0/1098/startcop.zip
SubSeven	Remote control trojan software	http://www.securityfocus.com/tools/1403
Sudo v1.6.3p7	Grants limited access to Unix privileges	http://www.rge.com/pub/admin/sudo/
SuperScan	A Windows-based port scanner	http://www.packetstormsecurity.com
Swatch 3.0.4	Unix syslog monitoring tool	ftp://ftp.stanford.edu/general/security-tools/swatch/
Tcpdump	A packet sniffer for Linux	http://www.tcpdump.org
TCP Wrappers 7.6	Inetd wrapper program that monitors, logs, and controls access to network services	ftp://ftp.porcupine.org/pub/security/tcp_wrappers_7.6.tar.gz
TFN2K	A DDoS tool	http://www.packetstormsecurity.com
Tiny	Personal firewall	http://www.tinysoftware.com/
Firewall v2.0	for Windows-based systems	tiny/files/apps/pf2.exe
Tripwire	Host-based intrusion detection system that uses MD5 hashes of files to detect changes	http://www.tripwire.org/downloads/index.php
Webslueth	A Web site analysis tool	http://www.download.com
Whisker	A CGI scanner	http://www.wiretrip.net
Wildpackets's	Windows IP	http://www.wildpackets.com/

NOTES

Shareware and Freeware Security Tools Continued

Application	Description	Available At
IP Subnet Calculator	Subnet calculator	products/ipsubnetcalculator
Windump	A packet sniffer for Windows	http://www.netgroup-serv.polito.it/windump/install/Default.htm
Winnuke	A tool that causes Windows NT 4.0 servers SP 3 or earlier to perform a Blue Screen of Death	http://www.astalavista.com
WinZip 8.1	A Windows-based file archiving and compression tool	http://www.winzip.com
Xinetd 2.3.3	Inetd replacement that combines inetd and TCP wrappers	http://www.synack.net/xinetd/
ZoneAlarm Personal Firewall	Personal firewall for Windows-based systems	http://www.zonealarm.com/za_download_1.htm

In order to make the most out of this book and the tools on your network, you need to be running both Microsoft Windows 2000 and RedHat Linux. The easiest way to do this is to configure your system to dual-boot two different operating systems. The following section walks you through the steps needed to configure your system.

EXERCISE 1: CONFIGURING YOUR SYSTEM

Description

Throughout this book you will perform several exercises that use either Windows 2000 or Linux. To successfully perform these exercises, it is necessary to have access to systems running either Windows 2000 or Linux, or both. To minimize the investment required to set up your test lab, we will show you how to create a single system that can run either operating system.

This technique does not allow you to operate both operating systems simultaneously. To do that, you will need a product, such as VMware, that creates virtual machines to operate concurrently. Now that used systems are fairly cheap, ideally you could set up at least two computers to dual-boot. Then, you can boot either system into either operating system for maximum flexibility.

Both Windows 2000 and Linux are dynamic operating systems, and security patches are constantly published as new vulnerabilities are discovered. This is normally a good thing, but it can work against your ability to run this book's exercises successfully. A security patch might correct a problem that we are trying to demonstrate. For this reason, we strongly recommend that you set up a system as defined in this exercise. This ensures that you achieve the maximum value the activities in this book offer. Also even if an exercise doesn't work properly, you can still learn about the tools demonstrated. Thus, even if you have an existing system that has been patched, it is worth your time to run through each exercise.

Similarly, we emphasize that this is not how you should set up a production system. Lab systems are set up for learning. We are deliberately leaving vulnerabilities installed and unnecessary services running. Excellent references are available to assist with the setup of secure production systems. The SANS Institute has

several references to aid you, including the following guides: *Windows 2000 Security: Step-By-Step* and *Securing Linux: Step-By-Step*.

We also strongly recommend that you not connect the lab systems you set up for this book to a production network. You will be installing software that can be dangerous or that can reveal sensitive information. You should not risk exposing your valuable systems to these tools.

Finally, unless you are the owner of the system you will be setting up for these labs, you should get written permission from the system owner to install the software and perform the exercises in this book. Failure to do so could subject you to disciplinary action. Anyone who works in the field of network security should have a small, personal lab set up at home, where new exploits and tools can be tested without risking repercussions from an employer.

Requirements

- **Permission**

The exercises in this book entail the installation of malware that can provide complete control over a targeted system. If you are not the legal owner of the systems used for the exercises in this book, you should obtain authorization from the legal owner and/or your management team prior to conducting this or any other exercise. ***Do not proceed without receiving the necessary permissions.***

- **Hardware**

An Intel-based PC that meets the requirements of Windows 2000 as documented by Microsoft at <http://www.microsoft.com/windows2000/server/howtobuy/upgrading/compat/default.asp> and Red Hat Linux 7.2 as documented by Red Hat at <http://www.hardware.redhat.com/hcl/genpage2.cgi?pagename=hcl>

NOTES

- 4GB minimum hard disk drive
- 128MB RAM memory (256MB or greater is recommended)
- Ethernet adapter
- **Software**
 - Windows 2000 Professional
 - Red Hat Linux 7.2 Professional

Challenge Procedure

The following are the general steps that you are going to perform:

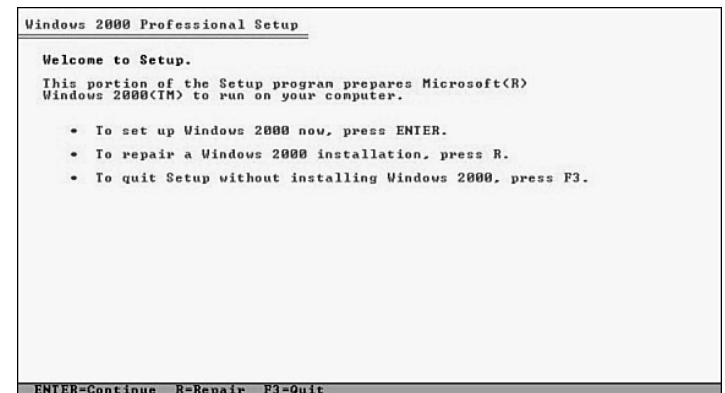
1. Install Windows 2000 Professional.
2. Install Red Hat Linux 7.2 Professional.
3. Test boot into each operating system.

Challenge Procedure Step-by-Step

The following are the exact steps you are going to perform to configure your system for dual-boot operating systems:

1. First, install Windows 2000 Professional. To do this, power on the PC and insert the Windows 2000 Professional installation CD. The system should boot off of the CD. If it does, proceed to step 3. If your system does not boot from the CD, check the PC BIOS settings to verify that it is set up to do so. It is a good security procedure to disable this feature, and it may have been disabled on your PC. If your PC does not support booting from the CD, you will need to perform step 2 to create boot disks.
2. Label four blank, formatted, 3.5-inch, 1.44MB floppy disks: **Setup Disk One**, **Setup Disk Two**, **Setup Disk Three**, and **Setup Disk Four**.
3. Insert **Setup Disk One** into the floppy disk drive of any Windows or DOS system.

4. Insert the Windows 2000 CD-ROM into the CD-ROM drive.
5. Click **Start**, and then click **Run**. In the **Open** box, type the following:
d:\bootdisk\makeboot a:
d: is the drive letter assigned to your CD-ROM drive. Click **OK**.
6. Follow the screen prompts. Then, insert **Setup Disk One** in the floppy disk drive of the lab PC and power the PC on.
7. After processing for a while, the following screen should appear. Press **Enter** to install Windows 2000.



8. Press C to continue with the installation.

```
Windows 2000 Professional Setup

Setup has determined that your computer's startup hard disk is new
or has been erased, or that your computer is running an operating
system that is incompatible with Windows 2000.

If the hard disk is new or has been erased, or if you want to discard
its current contents, you can choose to continue Setup.

If your computer is running an operating system that is incompatible
with Windows 2000, continuing Setup may damage or destroy the existing
operating system.

• To continue Setup, press C.
  CAUTION: Any data currently on your computer's startup hard disk
  will be lost.
• To quit Setup, press F3.

C-Continue Setup  F3-Quit
```

9. Review the license agreement and press F8 to accept it.

```
Windows 2000 Licensing Agreement

*****
Microsoft Windows 2000 Professional Licensed Copies: 1
*****
END-USER LICENSE AGREEMENT
*****

IMPORTANT-READ CAREFULLY: This End-User License Agreement
("EULA") is a legal agreement between you (either an
individual or a single entity) and Microsoft Corporation for
the Microsoft software product identified above, which
includes computer software and may include associated media,
printed materials, and "online" or electronic documentation
("Product"). An amendment or addendum to this EULA may
accompany the Product. YOU AGREE TO BE BOUND
BY THE TERMS OF THIS EULA BY INSTALLING,
COPYING, OR OTHERWISE USING THE PRODUCT. IF
YOU DO NOT AGREE, DO NOT INSTALL OR USE THE
PRODUCT; YOU MAY RETURN IT TO YOUR PLACE OF
PURCHASE FOR A FULL REFUND.

1. GRANT OF LICENSE. Microsoft grants you the following
rights provided that you comply with all terms and
conditions of this EULA:

* Installation and use. You may install, use, access,

F8-I agree  ESC-I do not agree  PAGE DOWN-Next Page
```

10. Press C to create a partition in the unpartitioned disk space.

```
Windows 2000 Professional Setup

The following list shows the existing partitions and
unpartitioned space on this computer.

Use the UP and DOWN ARROW keys to select an item in the list.

• To set up Windows 2000 on the selected item, press ENTER.
• To create a partition in the unpartitioned space, press C.
• To delete the selected partition, press D.

4895 MB Disk 0 at Id 0 on bus 0 on atapi
  Unpartitioned space  4895 MB

ENTER=Install  C=Create Partition  F3=Quit
```

11. Create a partition that is at least 2,000MB (2GB).

```
Windows 2000 Professional Setup

You asked Setup to create a new partition on
4895 MB Disk 0 at Id 0 on bus 0 on atapi.

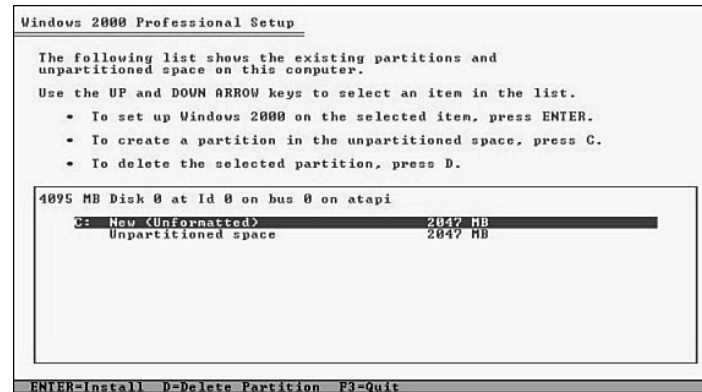
• To create the new partition, enter a size below and
  press ENTER.
• To go back to the previous screen without creating
  the partition, press ESC.

The minimum size for the new partition is      8 megabytes (MB).
The maximum size for the new partition is 4887 megabytes (MB).
Create partition of size (in MB): 2000

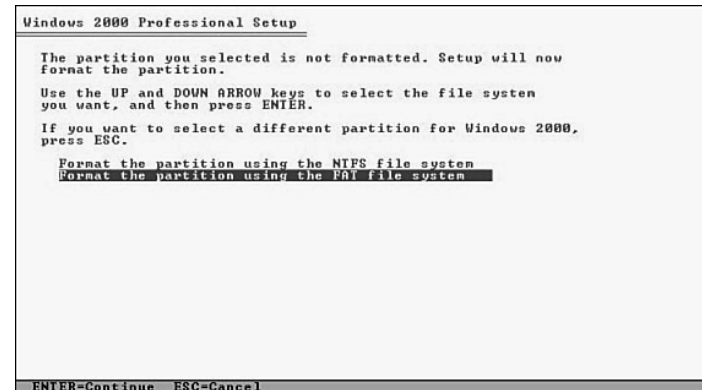
ENTER=Create  ESC=Cancel
```

NOTES

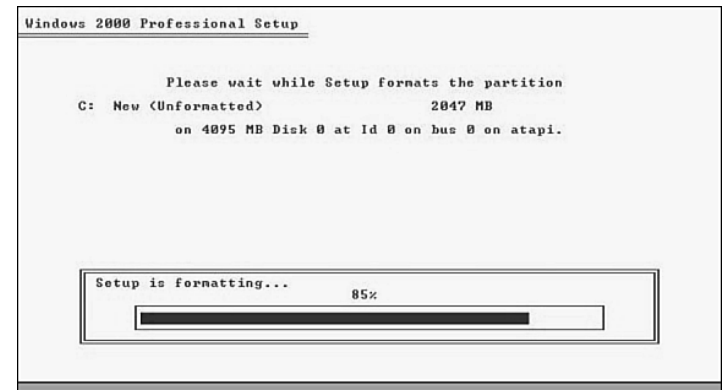
12. You are taken back to the main partition selection screen. Select the C: partition and press **Enter**.



13. Select **Format the Partition Using the FAT File System** and press **Enter**.



14. A progress bar displays.



15. After the disk is formatted, the setup routine copies the initial files to the system.



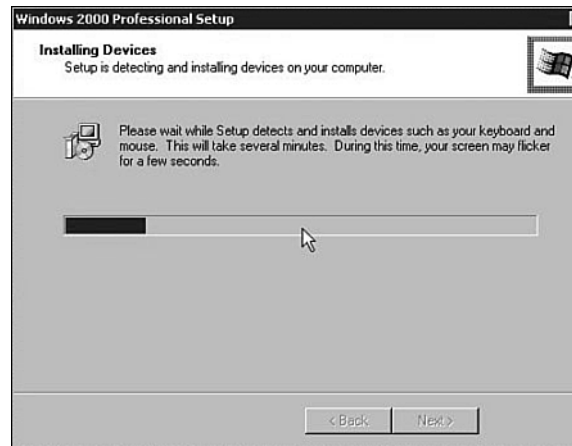
16. After the initial installation files have been copied to the new system, press **Enter** to reboot the system. It automatically reboots after about 15 seconds. If you booted off floppies, be sure to remove them from the disk drive before rebooting.



17. When the system reboots, the Windows 2000 Setup Wizard automatically starts. Click **Next** to continue.



18. The Setup Wizard attempts to detect the devices on your system. Click **Next** to proceed.

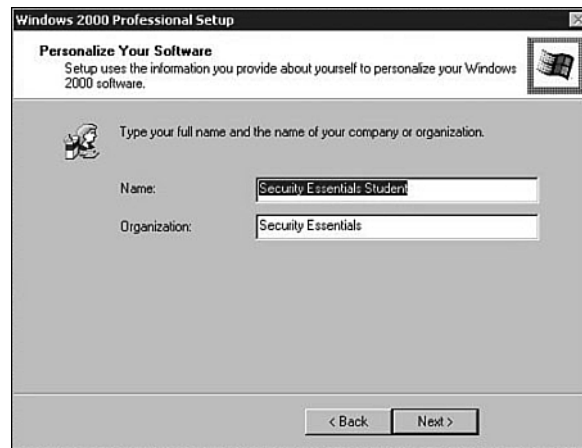


19. The installation process defaults to the English (United States) locale with the US keyboard layout. Click **Next** to accept the defaults. The **Regional Settings** screen appears.

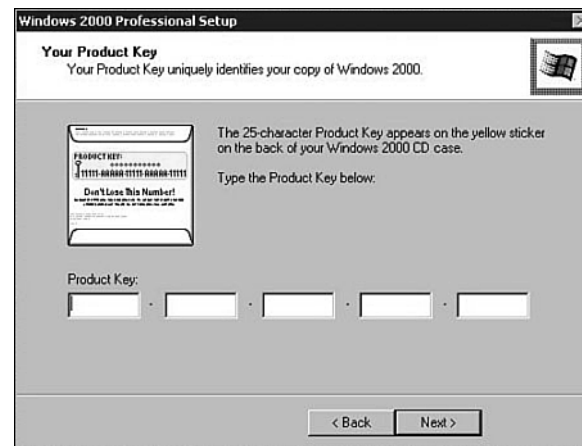


NOTES

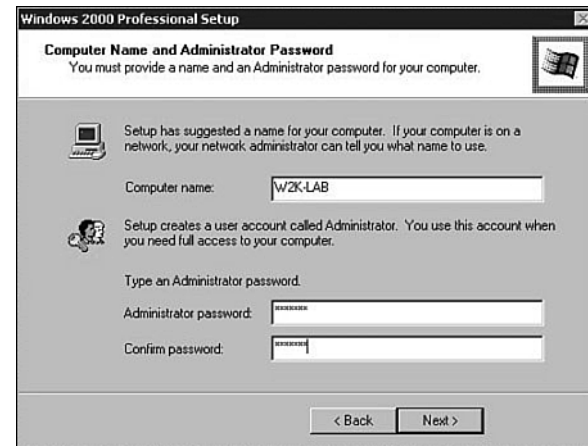
20. Enter an account name and organization to personalize your software. The **Personalize Your Software** screen appears. Click **Next**.



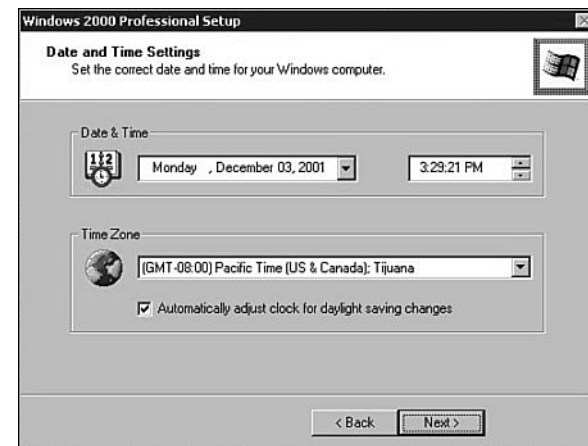
21. The **Your Product Key** screen appears. Enter the product key that came with your Windows 2000 distribution. Click **Next**.



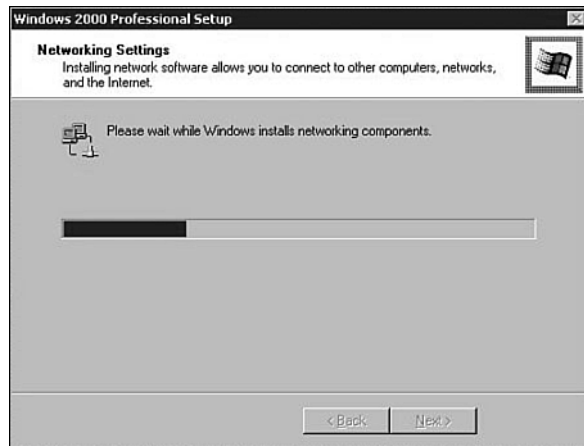
22. The **Computer Name and Administrator Password** screen appears. Give it a meaningful name and assign a strong password to the administrator account. Good passwords are at least eight characters in length and include upper- and lowercase letters, special characters, and numbers. Click **Next**.



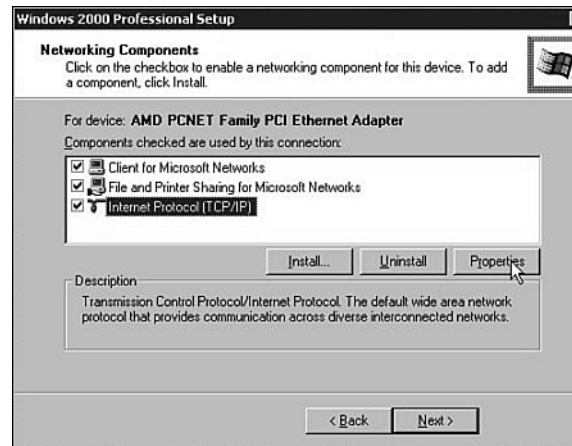
23. In the **Date and Time Settings** box, set the time zone to correspond to yours and adjust the date and time if necessary. Click **Next**.



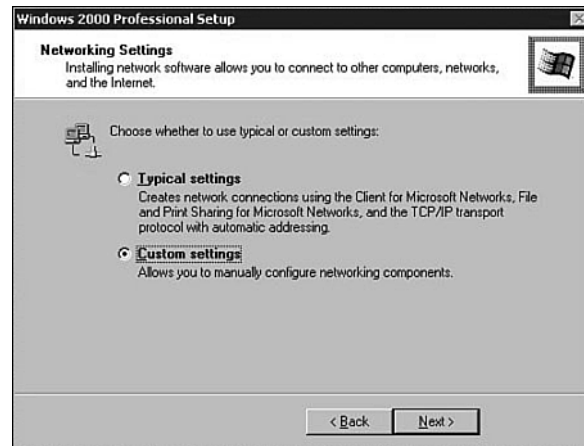
24. The wizard installs the networking software for your system.



26. In the **Networking Components** screen, double-click the **Internet Protocol (TCP/IP)**.



25. When prompted, click the **Custom Settings** radio button, and then click **Next**.

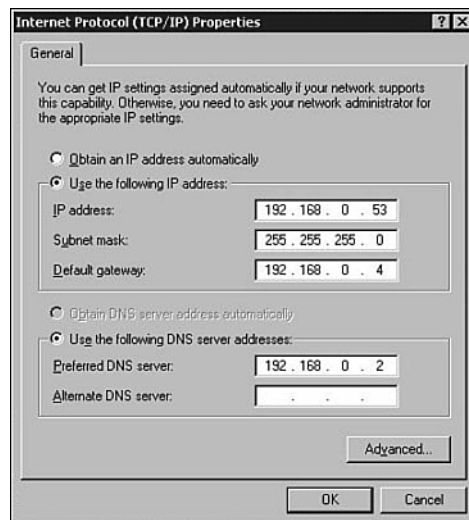


NOTES

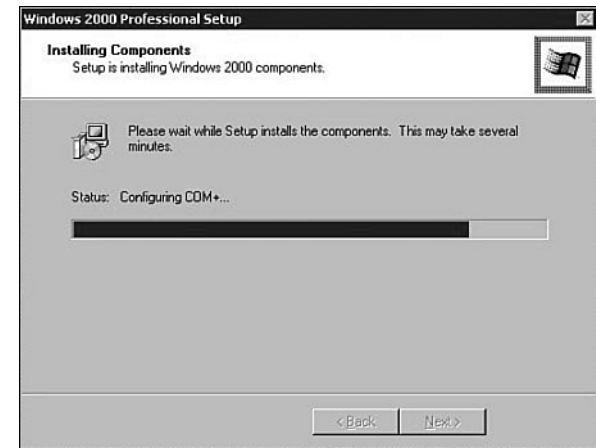
27. Enter the appropriate IP settings. Click **Use the Following IP Address** and **Use the Following DNS Server Addresses**. Enter the following values:

IP address: 192.168.0.53
Subnet mask: 255.255.255.0
Default gateway: 192.168.0.4
Preferred DNS server: 192.168.0.2

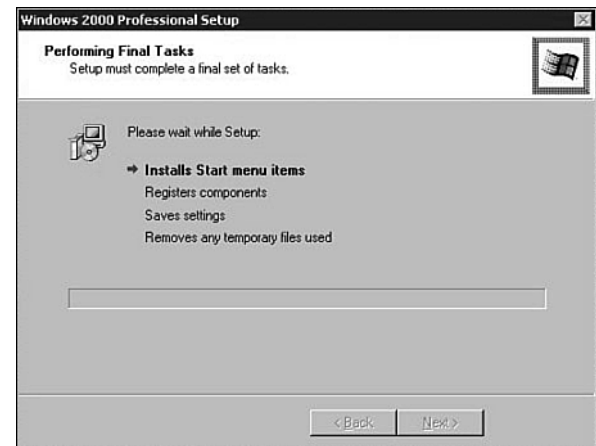
If you want to hook the system up to a network, use settings appropriate for your network. Click **OK** after you have entered the settings.



28. The system proceeds with the installation.



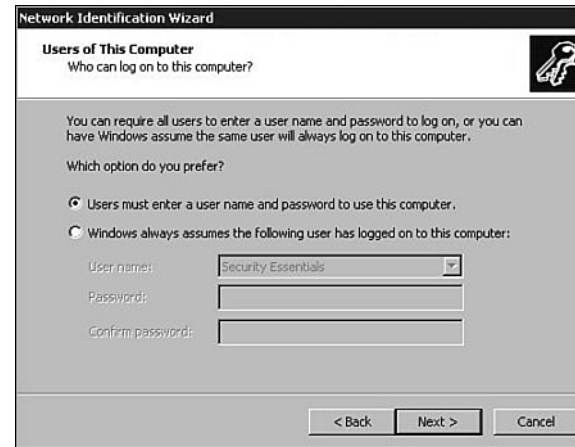
The Setup Wizard completes the installation by building the Start menu, registering installed components, and removing the temporary files it created.



29. The basic installation is completed. Remove the installation CD and click **Finish** to reboot the system.



31. Click the **Users Must Enter a Name and Password to Use This Computer** radio button, and then click **Next**.



30. The Network Identification Wizard automatically starts. Click **Next**.



32. Click **Finish** to complete the wizard.



NOTES

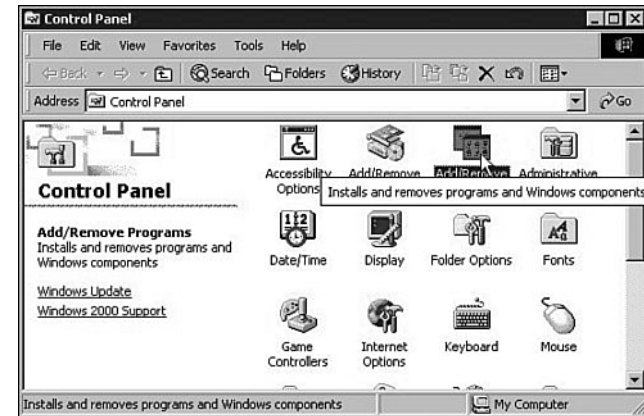
33. Log in to the system with the password you defined earlier.



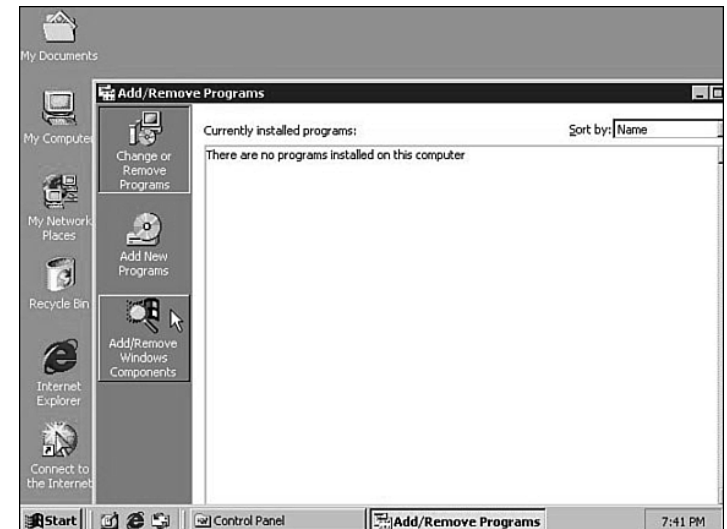
34. In the Getting Started With Windows 2000 screen, uncheck the **Show This Screen at Startup** check box and then click **Exit**.



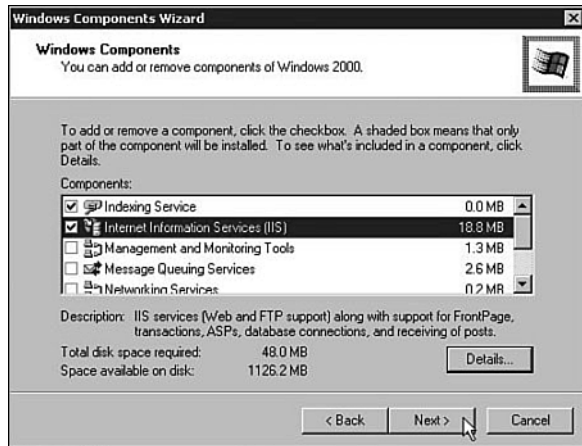
35. Select **Start, Settings, Control Panel**. Double-click **Add/Remove Programs**.



36. Click the **Add/Remove Windows Components** button.



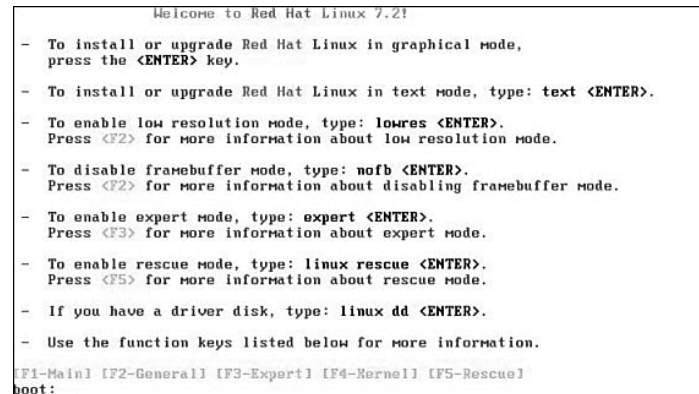
37. Click the **Internet Information Services (IIS)** check box, and then click **Next**.



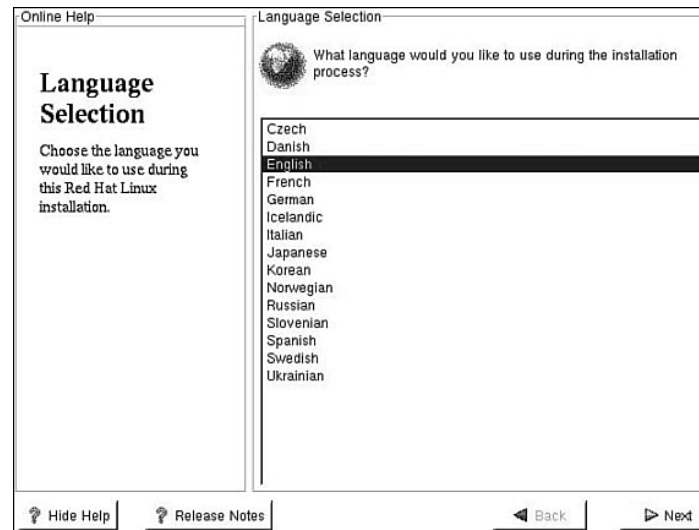
38. After the IIS installation has completed, remove the Windows CD and insert the Red Hat CD labeled **Red Hat Linux 7.1 Operating System CD 1**. Select **Start**, **Shutdown** and select **Restart** from the drop-down box. Click **OK** to restart the system, and you are done installing Windows 2000.



39. Next, install Red Hat Linux 7.2 Professional. The system will boot off the Red Hat Linux Installation CD and give you an installation choice menu. Press the **Enter** key to start the Linux installation process. If necessary, use the boot disk provided with the Red Hat distribution.

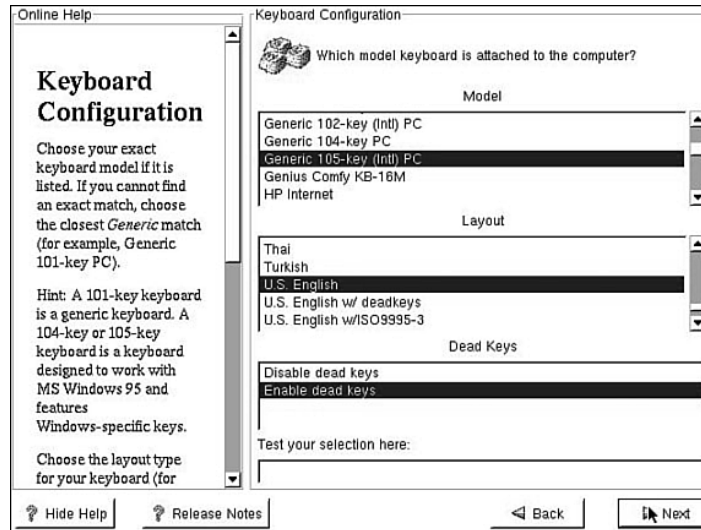


40. When the **Language Selection** screen appears, click **English**, and then click **Next**.

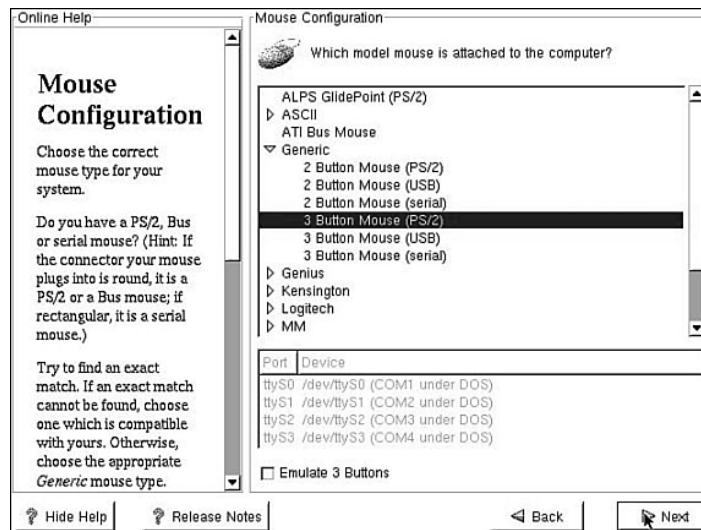


NOTES

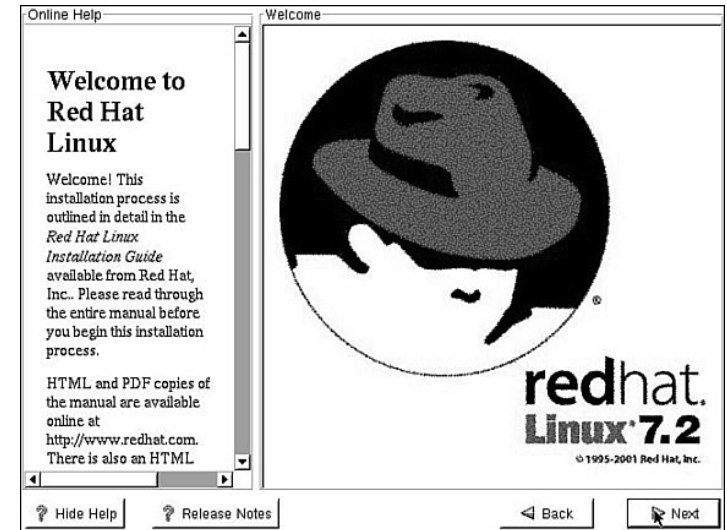
41. Accept the default keyboard configuration options and click **Next**.



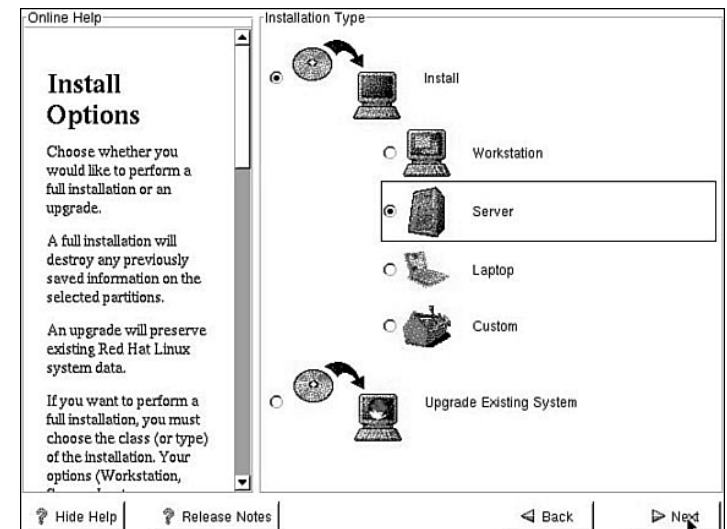
42. Accept the default mouse configuration and click **Next**.



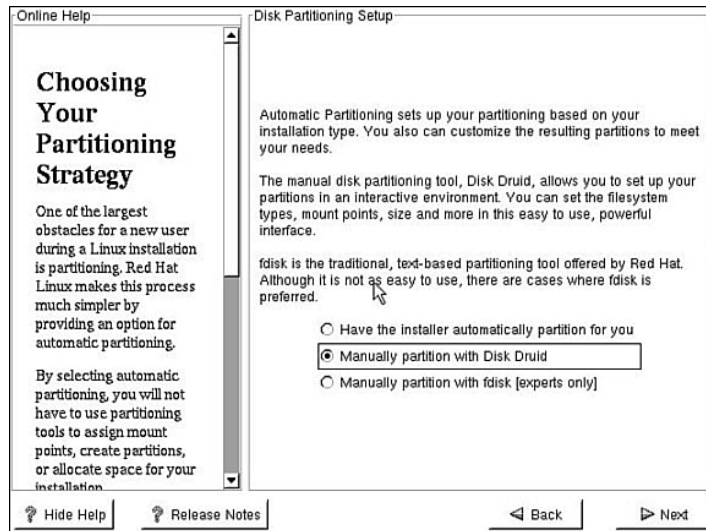
43. In the **Welcome to Red Hat Linux** screen, click **Next** to continue.



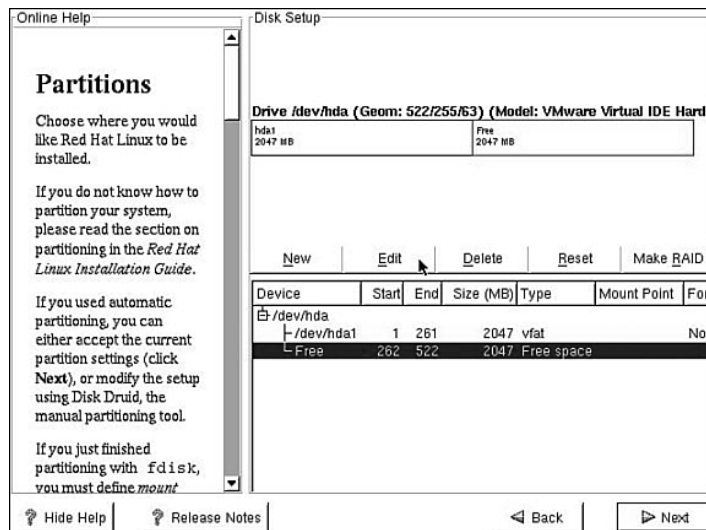
44. Click the **Server** radio button, and then click the **Next** button to do a basic server installation.



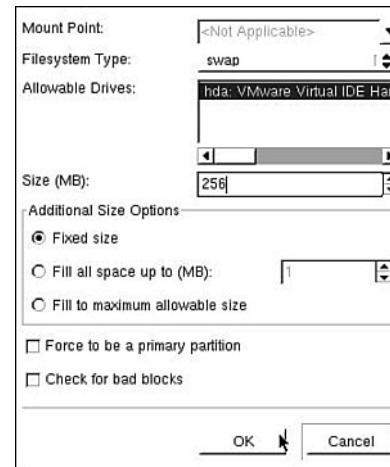
45. Click the **Manually Partition with Disk Druid** radio button, and then click the **Next** button.



46. Click the **Free** partition, and click **Next**.

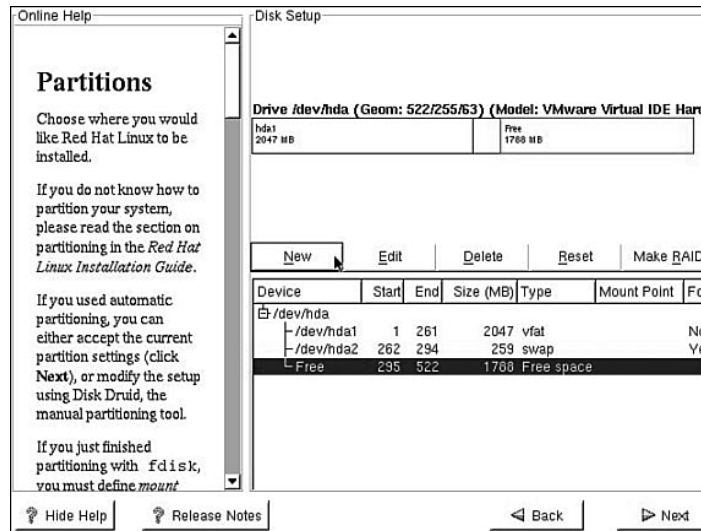


47. On the **Filesystem Type:** list box, select **swap**. Enter an appropriate value into the **Size (MB)** text box. As a rule of thumb, the swap file should be twice the size of your system's memory. However, for this installation you should leave at least 1.5GB for the Linux partition. Click **Next** to proceed.

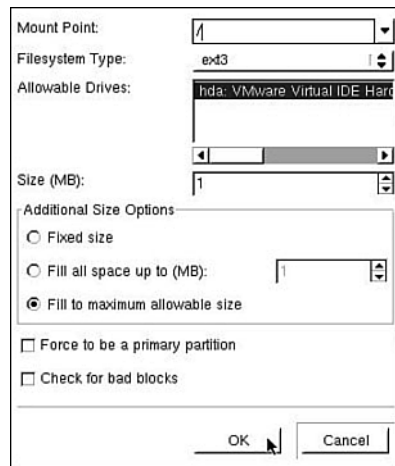


NOTES

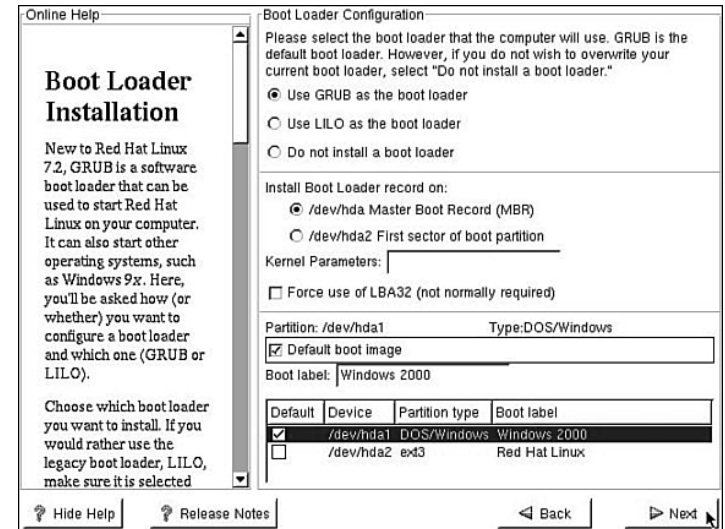
48. Click the **Free** partition, and then click the **New** button.



49. In the **Mount Point** drop-down box, select the root directory (/). Under the **Filesystem Type** list box, select **ext3**. Click the **Fill to Maximum Allowable Size** radio button. Click **OK** to accept the partition values. Finally, click **Next** to proceed.



50. Click the **Use GRUB as the Boot Loader** radio button. Select the **DOS** partition. In the **Boot Label:** text box, enter **Windows 2000**. If you want, you can set the system to boot into Windows 2000 by default by checking the **Default Boot Image** check box.



51. In the **GRUB Password** screen, click **Next** to proceed.

52. In the **Network Configuration** screen, uncheck the **Configure Using DHCP** check box. Enter the following values:

IP address: 192.168.0.54
 Netmask: 255.255.255.0
 Network: 192.168.0.0
 Broadcast: 192.168.0.255
 Hostname: Linux-Lab
 Gateway: 192.168.0.4
 Primary DNS: 192.168.0.2

53. In the **Firewall Configuration** screen, click the **Medium** and **Customize** radio buttons. Click the **eth0**, **SSH**, **Telnet**, **WWW (HTTP)**, **Mail (SMTP)**, and **FTP** check boxes.