

**100 NEW
HACKS**

LINUX SERVER HACKS™

Volume Two

*Tips & Tools for
Connecting, Monitoring,
and Troubleshooting*



O'REILLY®

*William von Hagen
& Brian K. Jones*

Linux Server Hacks, Volume Two

Table of Contents

[Credits](#)

[About the Authors](#)

[Contributors](#)

[Acknowledgments](#)

[Preface](#)

[Why Linux Server Hacks, Volume Two?](#)

[How to Use This Book](#)

[How This Book Is Organized](#)

[Conventions Used in This Book](#)

[Using Code Examples](#)

[How to Contact Us](#)

[Safari® Enabled](#)

[Got a Hack?](#)

[1. Linux Authentication](#)

[1.1. Hacks 1–9: Introduction](#)

[Hack #1. Disable User Accounts Instantly](#)

[1.2.1. Disabling Accounts on Systems That Use Local Authentication](#)

[1.2.2. Disabling Accounts on Systems That Use Distributed Authentication](#)

[Hack #2. Edit Your Password File for Greater Access Control](#)

[Hack #3. Deny All Access in One Second or Less](#)

[1.4.1. See Also](#)

[Hack #4. Customize Authentication with PAMs](#)

[1.5.1. PAM Overview](#)

[1.5.2. Per-Application/Service PAM Configuration Files](#)

[1.5.3. PAMs Used by the login Process](#)

[1.5.4. Configuration and More Configuration](#)

[1.5.5. What if PAM Configuration Files Are Missing?](#)

[1.5.6. See Also](#)

[Hack #5. Authenticate Linux Users with a Windows Domain Controller](#)

[1.6.1. Software Requirements](#)

[1.6.2. Critical Samba Configuration for Using Windows Authentication](#)

[1.6.3. Updating /etc/nsswitch.conf](#)

[1.6.4. Integrating the pam_winbind.so PAM into System Authentication](#)

[1.6.5. Starting the winbindd Daemon](#)

[1.6.6. Joining the Domain](#)

[1.6.7. Testing Windows Authentication](#)

[1.6.8. Debugging Windows Authentication Problems](#)

[1.6.9. See Also](#)

[Hack #6. Centralize Logins with LDAP](#)

[1.7.1. Installing LDAP Clients and Servers](#)

[1.7.2. Configuring an OpenLDAP Server](#)

[1.7.3. Migrating User, Password, and Group Entries to an LDAP Server](#)

[1.7.4. Updating Client Systems to Use LDAP Authentication](#)

[1.7.5. See Also](#)

[Hack #7. Secure Your System with Kerberos](#)

[1.8.1. Installing Kerberos](#)

[1.8.2. Installing and Configuring a Kerberos Server](#)

[1.8.3. Installing and Configuring Kerberos Clients and Applications](#)

[1.8.4. Using Kerberos for Login Authentication](#)

[1.8.5. See Also](#)

[Hack #8. Authenticate NFS-Lovers with NIS](#)

[1.9.1. Installing NIS Clients and Servers](#)

[1.9.2. Setting Up an NIS Server](#)

[1.9.3. Setting Up an NIS Client](#)

[1.9.4. See Also](#)

[Hack #9. Sync LDAP Data with NIS](#)

[1.10.1. The Code](#)

[1.10.2. Running the Code](#)

[1.10.3. See Also](#)

[2. Remote GUI Connectivity](#)

[2.1. Hacks 10–19: Introduction](#)

[Hack #10. Access Systems Remotely with VNC](#)

[2.2.1. Understanding the VNC Server Startup Process](#)

[2.2.2. Starting Your VNC Server](#)

[2.2.3. Connecting to a VNC Server](#)

[2.2.4. Customizing Your VNC Server's X Window System Environment](#)

[2.2.5. Stopping Your VNC Server](#)

[2.2.6. Optimizing VNC Performance](#)

[2.2.7. See Also](#)

[Hack #11. Access VNC Servers over the Web](#)

[2.3.1. Installing Java Classes and Associated Files for the VNC Server](#)

[2.3.2. See Also](#)

[Hack #12. Secure VNC via SSH](#)

[2.4.1. Forwarding Remote VNC Ports to Your Current Host](#)

[2.4.2. Public or Private VNC Forwarding](#)

[2.4.3. Forwarding Ports Without Remote Login](#)

[2.4.4. Improving Performance with Compression](#)

[2.4.5. Optimizing Graphical Updates Between Server and Viewer](#)

[2.4.6. See Also](#)

[Hack #13. Autostart VNC Servers on Demand](#)

[2.5.1. Integrating Xvnc with inetd or xinetd](#)

[2.5.2. Activating XDMCP](#)

[2.5.3. Starting the Viewer](#)

[2.5.4. Troubleshooting Xvnc Startup](#)

[2.5.5. See Also](#)

[Hack #14. Put Your Desktops on a Thin Client Diet](#)

[2.6.1. Understanding the LTSP Client Boot Process](#)

[2.6.2. Downloading and Installing the LTSP Software](#)

[2.6.3. Configuring and Starting the LTSP Server](#)

[2.6.4. Preparing LTSP Client Boot Media](#)

[2.6.5. Booting an LTSP Client](#)

[2.6.6. See Also](#)

[Hack #15. Run Windows over the Network](#)

[2.7.1. Opening Your Connection](#)

[2.7.2. Mapping Local Devices to Your Remote Session](#)

[2.7.3. See Also](#)

[Hack #16. Secure, Lightweight X Connections with FreeNX](#)

[2.8.1. Installing the FreeNX Server](#)

[2.8.2. Installing the NX Client](#)

[2.8.3. Configuring and Starting Your NX Client](#)

[2.8.4. See Also](#)

[Hack #17. Secure VNC Connections with FreeNX](#)

[2.9.1. Creating an NX Client Configuration for VNC](#)

[2.9.2. See Also](#)

[Hack #18. Secure Windows Terminal Connections with FreeNX](#)

[2.10.1. Creating an NX Client Configuration for a Windows Terminal Server](#)

[2.10.2. See Also](#)

[Hack #19. Remote Administration with Webmin](#)

[2.11.1. Installation](#)

[2.11.2. Configure Away!](#)

[2.11.3. See Also](#)

[3. System Services](#)

[3.1. Hacks 20–28: Introduction](#)

[Hack #20. Quick and Easy DHCP Setup](#)

[3.2.1. Installing a DHCP Server](#)

[3.2.2. Configuring Simple DHCP Services](#)

[3.2.3. Fire It Up!](#)

[3.2.4. See Also](#)

[Hack #21. Integrate DHCP and DNS with Dynamic DNS Updates](#)

[3.3.1. Configuring the BIND 9 Name Server](#)

[3.3.2. Configuring the ISC DHCP Server](#)

[3.3.3. Starting the Services and Troubleshooting](#)

[3.3.4. See Also](#)

[Hack #22. Synchronize Your Watches!](#)

[3.4.1. Hey! My Servers Are Gone!](#)

[3.4.2. See Also](#)

[Hack #23. Centralize X Window System Font Resources](#)

[3.5.1. Billions and Billions of Fonts...](#)

[3.5.2. Setting Up an X Font Server](#)

[3.5.3. Copying Fonts to a Font Server](#)

[3.5.4. Starting or Restarting the X Font Server](#)

[3.5.5. Updating Desktop Systems to Use an X Font Server](#)

[3.5.6. Troubleshooting](#)

[3.5.7. Summary](#)

[3.5.8. See Also](#)

[Hack #24. Create a CUPS Print Server](#)

[3.6.1. Defining a New Printer in CUPS](#)

[3.6.2. Testing CUPS Printing](#)

[3.6.3. Fine-Tuning Printer Configuration in CUPS](#)

[3.6.4. Enabling Remote Printing on the CUPS Server](#)

[3.6.5. Troubleshooting CUPS Printing](#)

[3.6.6. Summary](#)

[3.6.7. See Also](#)

[Hack #25. Configure Linux Connections to Remote CUPS Printers](#)

[3.7.1. Defining a Remote Printer in CUPS](#)

[3.7.2. Summary](#)

[3.7.3. See Also](#)

[Hack #26. Integrate Windows Printing with CUPS](#)

[3.8.1. Configuring Printing from Windows 2000/XP Systems](#)

[3.8.2. Server-Side Configuration for HTTP Printing](#)

[3.8.3. Troubleshooting Windows Printing to CUPS Servers](#)

[3.8.4. See Also](#)

[Hack #27. Centralize Macintosh Printing with CUPS](#)

[3.9.1. Configuring Access to a Remote CUPS Server](#)

[3.9.2. Server-Side Configuration for HTTP Printing](#)

[3.9.3. Testing Printing from Mac OS X to Your CUPS Server](#)

[3.9.4. Troubleshooting Mac OS X Printing to CUPS Servers](#)

[3.9.5. See Also](#)

[Hack #28. Define a Secure CUPS Printer](#)

[3.10.1. Enabling Remote Printing on a CUPS Server](#)

[3.10.2. Restricting Printer Access to Specific IP Addresses](#)

[3.10.3. Restricting Printer Access to Specific Users](#)

[3.10.4. Summary](#)

[3.10.5. See Also](#)

[4. Cool Sysadmin Tools and Tips](#)

[4.1. Hacks 29–45: Introduction](#)

[Hack #29. Execute Commands Simultaneously on Multiple Servers](#)

[4.2.1. See Also](#)

[Hack #30. Collaborate Safely with a Secured Wiki](#)

[4.3.1. Installing MediaWiki](#)

[4.3.2. Configuring MediaWiki](#)

[4.3.3. Getting Started: Data Structure](#)

[Hack #31. Edit Your GRUB Configuration with grubby](#)

[Hack #32. Give Your Tab Key a Workout](#)

[4.5.1. See Also](#)

[Hack #33. Keep Processes Running After a Shell Exits](#)

[4.6.1. Using nohup to Execute Commands](#)

[4.6.2. Using disown with Background Jobs](#)

[4.6.3. See Also](#)

[Hack #34. Disconnect Your Console Without Ending Your Session](#)

[4.7.1. screen Scripting](#)

[4.7.2. See Also](#)

[Hack #35. Use script to Save Yourself Time and Train Others](#)

[4.8.1. See Also](#)

[Hack #36. Install Linux Simply by Booting](#)

[4.9.1. Preparatory Steps](#)

[4.9.2. Getting It Working](#)

[4.9.3. Quick Troubleshooting](#)

[Hack #37. Turn Your Laptop into a Makeshift Console](#)

[4.10.1. Introducing minicom](#)

[4.10.2. Testing It](#)

[4.10.3. Troubleshooting](#)

[Hack #38. Usable Documentation for the Inherently Lazy](#)

[Hack #39. Exploit the Power of Vim](#)

[4.12.1. Recording a Vim Macro](#)

[4.12.2. Creating Vim Shortcut Keys](#)

[Hack #40. Move Your PHP Web Scripting Skills to the Command Line](#)

[4.13.1. The Code](#)

[4.13.2. Running the Code](#)

[Hack #41. Enable Quick telnet/SSH Connections from the Desktop](#)

[4.14.1. See Also](#)

[Hack #42. Speed Up Compiles](#)

[4.15.1. Using distcc](#)

[4.15.2. Distribute Compiles to Windows Machines](#)

[Hack #43. Avoid Common Junior Mistakes](#)

[4.16.1. Don't Take the root Name in Vain](#)

[4.16.2. Don't Get Too Comfortable](#)

[4.16.3. Don't Perform Production Commands "Off the Cuff"](#)

[4.16.4. Ask Questions](#)

[Hack #44. Get Linux Past the Gatekeeper](#)

[4.17.1. Don't Talk Money](#)

[4.17.2. Don't Talk About Linux in a Vacuum](#)

[4.17.3. Don't Pitch Linux for Something It's Not Well Suited For](#)

[4.17.4. Don't Be Impatient](#)

[Hack #45. Prioritize Your Work](#)

[4.18.1. Prioritizing Tasks](#)

[4.18.2. Prioritizing Projects](#)

[4.18.3. Summary](#)

[5. Storage Management and Backups](#)

[5.1. Hacks 46–55: Introduction](#)

[Hack #46. Create Flexible Storage with LVM](#)

[5.2.1. Logical Volume Buzzwords](#)

[5.2.2. Allocating Physical Volumes](#)

[5.2.3. Assigning Physical Volumes to Volume Groups](#)

[5.2.4. Creating a Logical Volume from a Volume Group](#)

[5.2.5. Suggestions](#)

[5.2.6. See Also](#)

[Hack #47. Combine LVM and Software RAID](#)

[5.3.1. Mirroring and Redundancy](#)

[5.3.2. Overview of RAID Levels](#)

[5.3.3. Combining Software RAID and LVM](#)

[5.3.4. Creating RAID Devices](#)

[5.3.5. Combining RAID and LVM](#)

[5.3.6. See Also](#)

[Hack #48. Create a Copy-on-Write Snapshot of an LVM Volume](#)

[5.4.1. Kernel Support for Snapshots](#)

[5.4.2. Creating a Snapshot](#)

[5.4.3. Mounting a Snapshot](#)

[5.4.4. See Also](#)

[Hack #49. Clone Systems Quickly and Easily](#)

[5.5.1. Building partimage](#)

[5.5.2. Cloning Partitions Using partimage](#)

[5.5.3. Restoring Partitions Using partimage](#)

[5.5.4. Summary](#)

[5.5.5. See Also](#)

[Hack #50. Make Disk-to-Disk Backups for Large Drives](#)

[5.6.1. Convenient Removable Media Technologies for Backups](#)

[5.6.2. Choosing the Right Backup Command](#)

[5.6.3. The Code](#)

[5.6.4. Running the Code](#)

[5.6.5. Choosing What to Back Up](#)

[5.6.6. Summary and Tips](#)

[Hack #51. Free Up Disk Space Now](#)

[Hack #52. Share Files Using Linux Groups](#)

[5.8.1. Linux Protections 101](#)

[5.8.2. Setting the umask to Create Sharable Files](#)

[5.8.3. Using Directory Permissions to Set Group Membership](#)

[5.8.4. See Also](#)

[Hack #53. Refine Permissions with ACLs](#)

[5.9.1. Installing and Activating ACL Support](#)

[5.9.2. Overview of Linux ACLs and Utilities](#)

[5.9.3. Displaying Current ACLs](#)

[5.9.4. Setting ACLs](#)

[5.9.5. See Also](#)

[Hack #54. Make Files Easier to Find with Extended Attributes](#)

[5.10.1. Getting and Installing Extended Attribute Support](#)

[5.10.2. Displaying Extended Attributes and Their Values](#)

[5.10.3. Setting Extended Attributes](#)

[5.10.4. Removing Extended Attributes](#)

[5.10.5. Searching Using Extended Attributes](#)

[Hack #55. Prevent Disk Hogs with Quotas](#)

[5.11.1. Setting Up Disk Quotas](#)

[5.11.2. Installing the Quota Software](#)

[5.11.3. Entering Single-User Mode](#)

[5.11.4. Editing /etc/fstab](#)

[5.11.5. Initializing the Quota Configuration Files](#)

[5.11.6. Configuring Your Quotas](#)

[5.11.7. See Also](#)

[6. Standardizing, Sharing, and Synchronizing Resources](#)

[6.1. Hacks 56–62: Introduction](#)

[Hack #56. Centralize Resources Using NFS](#)

[6.2.1. Configuring the NFS Server](#)

[6.2.2. Configuring the NFS Clients](#)

[6.2.3. Configuring the Service](#)

[6.2.4. A Final Consideration](#)

[Hack #57. Automount NFS Home Directories with autofs](#)

[Hack #58. Keep Filesystems Handy, but Out of Your Way](#)

[6.4.1. amd Configuration in a Nutshell](#)

[Hack #59. Synchronize root Environments with rsync](#)

[6.5.1. See Also](#)

[Hack #60. Share Files Across Platforms Using Samba](#)

[6.6.1. Setting Up Simple Samba Shares](#)

[Hack #61. Quick and Dirty NAS](#)

[6.7.1. Selecting the Hardware](#)

[6.7.2. Installing and Configuring Linux](#)

[6.7.3. Configuring User Storage](#)

[6.7.4. Configuring System Services](#)

[6.7.5. Deploying NAS Storage](#)

[6.7.6. Summary](#)

[6.7.7. See Also](#)

[Hack #62. Share Files and Directories over the Web](#)

[6.8.1. Installing and Configuring Apache's WebDAV Support](#)

[6.8.2. Creating WebDAV Users and Directories](#)

[6.8.3. See Also](#)

[7. Security](#)

[7.1. Hacks 63–68: Introduction](#)

[Hack #63. Increase Security by Disabling Unnecessary Services](#)

[7.2.1. Examining /etc/inittab](#)

[7.2.2. Optimizing Per-Runlevel Startup Scripts](#)

[7.2.3. Streamlining Services Run by the Internet Daemon](#)

[7.2.4. Summary](#)

[Hack #64. Allow or Deny Access by IP Address](#)

[7.3.1. Protecting Your Machine with hosts.allow and hosts.deny](#)

[7.3.2. Configuring hosts.allow and hosts.deny for Use](#)

[7.3.3. Hacking the Hack](#)

[7.3.4. See Also](#)

[Hack #65. Detect Network Intruders with snort](#)

[7.4.1. Installing snort](#)

[7.4.2. Configuring snort](#)

[7.4.3. Starting snort](#)

[7.4.4. Advanced snort](#)

[7.4.5. Summary](#)

[7.4.6. See Also](#)

[Hack #66. Tame Tripwire](#)

[7.5.1. Installing Tripwire](#)

[7.5.2. Tripwire's Execution Configuration File](#)

[7.5.3. Tripwire's Policy Configuration File](#)

[7.5.4. Preparing Tripwire for Use](#)

[7.5.5. Running Your First Filesystem Integrity Check](#)

[7.5.6. TripWire Tips](#)

[Hack #67. Verify Filesystem Integrity with Afick](#)

[7.6.1. Installing Afick](#)

[7.6.2. Configuring Afick to Match Your System](#)

[7.6.3. Running Afick](#)

[7.6.4. Securing Afick](#)

[7.6.5. Updating Your Database](#)

[7.6.6. Conclusion](#)

[7.6.7. See Also](#)

[Hack #68. Check for Rootkits and Other Attacks](#)

[7.7.1. Types of Rootkits](#)

[7.7.2. Obtaining, Building, and Installing chkrootkit](#)

[7.7.3. Running chkrootkit](#)

[7.7.4. Automating chkrootkit](#)

[7.7.5. Summary](#)

[7.7.6. See Also](#)

[8. Troubleshooting and Performance](#)

[8.1. Hacks 69–77: Introduction](#)

[Hack #69. Find Resource Hogs with Standard Commands](#)

[8.2.1. What About Disk Hogs?](#)

[8.2.2. Bandwidth Hogging](#)

[Hack #70. Reduce Restart Times with Journaling Filesystems](#)

[8.3.1. Journaling Filesystems 101](#)

[8.3.2. Journaling Filesystems Under Linux](#)

[8.3.3. Converting Existing Filesystems to Journaling Filesystems](#)

[8.3.4. Summary](#)

[8.3.5. See Also](#)

[Hack #71. Grok and Optimize Your System with sysctl](#)

[Hack #72. Get the Big Picture with Multiple Displays](#)

[8.5.1. See Also](#)

[Hack #73. Maximize Resources with a Minimalist Window Manager](#)

[8.6.1. Getting and Installing Fluxbox](#)

[8.6.2. Start Me Up, Scotty!](#)

[8.6.3. Configure Fluxbox](#)

[8.6.4. The Slit](#)

[8.6.5. Make It Pretty!](#)

[8.6.6. Minimal Hassle](#)

[8.6.7. See Also](#)

[Hack #74. Profile Your Systems Using /proc](#)

[8.7.1. The Code](#)

[Hack #75. Kill Processes the Right Way](#)

[8.8.1. Killing Processes in the Right Order](#)

[8.8.2. Stopping and Restarting a Process](#)

[8.8.3. The Last Resort](#)

[8.8.4. See Also](#)

[Hack #76. Use a Serial Console for Centralized Access to Your Systems](#)

[8.9.1. The Options](#)

[8.9.2. Start at the Beginning: The Bootloader](#)

[8.9.3. Putting It All Together](#)

[8.9.4. Where to Go from Here](#)

[8.9.5. See Also](#)

[Hack #77. Clean Up NIS After Users Depart](#)

[8.10.1. The Code](#)

[8.10.2. Running the Code](#)

[9. Logfiles and Monitoring](#)

[9.1. Hacks 78–88: Introduction](#)

[Hack #78. Avoid Catastrophic Disk Failure](#)

[Hack #79. Monitor Network Traffic with MRTG](#)

[9.3.1. Requirements](#)

[9.3.2. Installation](#)

[9.3.3. Automating MRTG](#)

[9.3.4. See Also](#)

[Hack #80. Keep a Constant Watch on Hosts](#)

[Hack #81. Remotely Monitor and Configure a Variety of Networked Equipment](#)

[9.5.1. The Code](#)

[9.5.2. Running the Code](#)

[Hack #82. Force Standalone Apps to Use syslog](#)

[Hack #83. Monitor Your Logfiles](#)

[9.7.1. Using log-guardian](#)

[9.7.2. Using logcheck](#)

[Hack #84. Send Log Messages to Your Jabber Client](#)

[9.8.1. The Code](#)

[9.8.2. Running the Code](#)

[Hack #85. Monitor Service Availability with Zabbix](#)

[9.9.1. Dependencies](#)

[9.9.2. Installing Zabbix](#)

[9.9.3. Monitoring Hosts](#)

[9.9.4. Mapping the Network](#)

[9.9.5. The Details](#)

[Hack #86. Fine-Tune the syslog Daemon](#)

[9.10.1. Making Sense of syslog.conf](#)

[9.10.2. Real-Time Alerts from the System Log](#)

[9.10.3. Centralizing Logs for Convenient Access](#)

[9.10.4. See Also](#)

[Hack #87. Centralize System Logs Securely](#)

[9.11.1. Getting Started](#)

[9.11.2. Creating Your Encryption Certificates](#)

[9.11.3. Configuring stunnel](#)

[9.11.4. Configuring syslog-ng](#)

[9.11.5. Testing](#)

[9.11.6. Where Next?](#)

[9.11.7. See Also](#)

[Hack #88. Keep Tabs on Systems and Services](#)

[9.12.1. Enter Nagios](#)

[9.12.2. Hosts, Services, and Contacts, Oh My!](#)

[9.12.3. See Also](#)

[10. System Rescue, Recovery, and Repair](#)

[10.1. Hacks 89–100: Introduction](#)

[Hack #89. Resolve Common Boot and Startup Problems](#)

[10.2.1. Check BIOS Settings](#)

[10.2.2. Fixing Runlevel or X Window System Problems](#)

[10.2.3. Regenerating a Default X Window System Configuration File](#)

[10.2.4. Booting to Single-User Mode](#)

[10.2.5. Resolving Filesystem Consistency Problems](#)

[10.2.6. See Also](#)

[Hack #90. Rescue Me!](#)

[10.3.1. Downloading and Burning the Rescue Disk](#)

[10.3.2. Using the Rescue CD](#)

[10.3.3. See Also](#)

[Hack #91. Bypass the Standard Init Sequence for Quick Repairs](#)

[Hack #92. Find Out Why You Can't Unmount a Partition](#)

[10.5.1. Background](#)

[10.5.2. Finding Processes That Are Using a Filesystem](#)

[10.5.3. Listing Open Files](#)

[10.5.4. Summary](#)

[10.5.5. See Also](#)

[Hack #93. Recover Lost Partitions](#)

[10.6.1. Looking for Partitions](#)

[10.6.2. Writing the Partition Table](#)

[10.6.3. See Also](#)

[Hack #94. Recover Data from Crashed Disks](#)

[10.7.1. Popular Disk Failure Modes](#)

[10.7.2. Attempt to Read Block from Filesystem Resulted in Short Read...](#)

[10.7.3. Standard Filesystem Diagnostics and Repair](#)

[10.7.4. Removing an ext3 Filesystem's Journal](#)

[10.7.5. Cloning a Bad Disk Using ddrescue](#)

[10.7.6. Checking the Restored Disk](#)

[10.7.7. See Also](#)

[Hack #95. Repair and Recover ReiserFS Filesystems](#)

[10.8.1. Correcting a Damaged ReiserFS Filesystem](#)

[10.8.2. Identifying Files and Directories in the ReiserFS lost+found](#)

[10.8.3. See Also](#)

[Hack #96. Piece Together Data from the lost+found](#)

[10.9.1. Exploring the lost+found](#)

[10.9.2. Recovering Directories from the lost+found](#)

[10.9.3. Recovering Recognizable Groups of Files](#)

[10.9.4. Examining Individual Files](#)

[10.9.5. Summary](#)

[10.9.6. See Also](#)

[Hack #97. Recover Deleted Files](#)

[10.10.1. Preventing Additional Changes to the Partition](#)

[10.10.2. Looking for the Missing Data](#)

[10.10.3. See Also](#)

[Hack #98. Permanently Delete Files](#)

[10.11.1. Using the shred Utility](#)

[10.11.2. See Also](#)

[Hack #99. Permanently Erase Hard Disks](#)

[10.12.1. Using shred to Wipe Hard Drives](#)

[10.12.2. Using Darik's Boot and Nuke](#)

[10.12.3. Summary](#)

[10.12.4. See Also](#)

[Hack #100. Recover Lost Files and Perform Forensic Analysis](#)

[10.13.1. Building and Installing The Sleuth Kit](#)

[10.13.2. Building and Installing Autopsy and Related Software](#)

[10.13.3. Using The Sleuth Kit to Recover Deleted Files](#)

[10.13.4. Summary](#)

[10.13.5. See Also](#)

Linux Server Hacks, Volume Two

William von Hagen

Brian K. Jones

Editor

David Brickner

Copyright © 2009 O'Reilly Media, Inc.

O'REILLY®

O'Reilly Media

Credits

About the Authors

Bill von Hagen has been a Unix system administrator for 20 years and a Linux fanatic since 1993. He has also worked as a systems programmer, product manager, writer, application developer, drummer and content manager.

Bill has written or cowritten books on such topics as Linux filesystems, SUSE Linux, Red Hat Linux, GCC, SGML, Mac OS X, Linux system administration, and hacking the TiVo. He has written numerous articles on Linux, Unix, and open source topics for publications including *Linux Magazine*, *Linux Journal*, *Linux Format*, and *Mac Format*. An avid computer collector specializing in workstations, he owns more than 200 computer systems and wants more. You can reach him at vonhagen@vonhagen.org.

Brian K. Jones (Jonesy) has been a Unix and Linux system and network administrator for six years. He has also held positions and consulted in the capacity of database administrator, web developer, project manager, instructional speaker, technical writer and editor, and studio musician, for clients large and small.

In the past, Brian has written extensively on topics revolving around Linux and open source software for Linux.com, *Newsforge*, and *Linux Magazine*, and he has served as author and Editor-in-Chief of *php|architect* magazine. In his copious free time (right), Brian enjoys playing billiards and guitar, woodworking, and writing code. He has worked as a system and network administrator for the computer science department at Princeton University since 2001, and as a part-time infrastructure computing consultant since 2000. You can reach him at jonesy@linuxlaboratory.org.

Contributors

The following people contributed their writing, code, and inspiration to *Linux Server Hacks, Volume Two*:

- Jon Fox [[Hacks #33](#) and [#62](#)] (jon.fox@gnu.org.uk) is a Linux user and free software advocate. He's been using Linux since 1996.
- Tom Limoncelli [[Hack #45](#)] has over 15 years of system administration experience and has been teaching workshops on time management at conferences since 2003. Tom has authored *Time Management for System Administrators* (O'Reilly) and *The Practice of System and Network Administration* (Addison Wesley). Outside of work, Tom has won awards for his activism in gay/bi/lesbian rights and now helps progressive causes to use technology to further their goals.
- Lance Tost has been a Linux user since the 0.98 kernel days, while he earned his B.S. in Computer Science. He has held programming, DBA, and, Unix administration positions. Lance is a Red Hat Certified Engineer as well as a Solaris Certified System Administrator. Lance contributed [[Hacks #29](#), [#41](#), [#48](#), [#59](#), [#63](#), and [#72](#)].
- Brian Warshawsky is an enthusiastic proponent of all things Linux and open source. His main interests include security, wireless networking, and finding new applications for the Linux operating system. By day he is a professional Unix/Linux system administrator, and by night he is a technical writer and avid mountain biker. He lives in Virginia with his soon-to-be wife Jennifer, his loyal dog Max, and his much less loyal cat Jackie. Brian contributed [[Hacks #19](#), [#55](#), [#64](#), [#66](#), [#67](#), [#73](#), [#75](#), [#76](#), [#79](#), [#85](#), [#86](#), and [#87](#)].
- David Brickner [[Hack #42](#)] is not a Linux server administrator, but as a Gentoo user, he has learned a couple of things about compiling software. David believes Linux will be the dominant desktop operating system in the near future, and to encourage its adoption, he has written *Test Driving Linux* and *Linux Desktop Pocket Guide*, both from O'Reilly.

Acknowledgments

Bill: For my wife, Dorothy Fisher, without whom life wouldn't be anywhere near as good or as much fun, and for Mike Bauer, Bill Gausa, and Larry Weidman, who gave me many professional opportunities and encouraged me to expand my horizons. I'd also like to thank David Brickner, without whom I never would have finished this book (well, at least not this year) and for the opportunity to write for O'Reilly in general. Without David's suggestions, comments, and general support, this would be a lesser book.

Finally, no book having to do with GNU/Linux would be complete without thanking Richard Stallman, Linus Torvalds, and the open source community in general. I'd also like to thank my coauthor, Brian Jones, for making this book better than it would have been without him.

Brian: For my wife, Natasha, who has supported and encouraged me in all of my ambitions and goals and has dealt with my nonsense while in pursuit of said ambitions and goals. Also for my siblings: Heather, for forcing me to pursue computing as a career; Jessica, for being almost sickeningly positive and encouraging; Jon, for keeping me on my toes; and Russell, without whom I might've self-destructed long ago.

A hearty thanks goes to David Brickner, who offered me the opportunity to write for O'Reilly, and whose even keel, firm hand, and sheer diligence have made this a wonderful experience. I'd also like to thank all the folks at OSTG, TriLUG, and php|architect, for being friends of mine; Matt Appio, for making me take occasional fishing breaks; and my coworkers at Princeton, for teaching me far more than I could ever list here.

To Linus Torvalds and the rest of the open source community: thank you so much for all your work.

Preface

Both authors of this book have been system administrators for a while. When the opportunity to write this book came about, we initially focused on cool hacks we'd developed or used in our server and system administration careers. We also asked friends, who asked their friends, and we were therefore able to get some great contributions from others to augment the things that we'd come up with. Everybody has problems they like to solve. Bill likes distributed authentication, undeleting and recovering files, and tweaking filesystems in general. Brian likes making admin tasks more efficient, reliable, and repeatable; has a bucketload of cool scripts to do various tasks; and loves getting and using data from remote sources. And every sysadmin has favorite techniques for solving problems, so Hack is to Hacker as Cool Tip or Technique is to Server or System Administrator. Sysadmin hacks are essentially clever ways of approaching whatever problem you're trying to solve, whether it's figuring out how to recover lost data, trying to collect information from distributed clients in one place so that you can easily see the big picture or anything else that comes up.

As we worked on this book, thinking about cool server and sysadmin hacks mutated into thinking about general tips and tricks that we found useful to simplify our lives as system administrators. We also noticed that there weren't really any books available along the lines of "Things We Wish Previous System Administrators Had Told Us." Leaving aside obvious questions like "where is the key to the RAID array" and "what was the root password on *<insert hostname here>*," we decided to "hack the Hacks series" a bit and incorporate some general sysadmin information, tips, and tricks as another of this book's primary themes. This means that we provide a bit more background material than you ordinarily see in Hacks books. You're not going to hurt our feelings if you skip over things you already know, but we hope that all the material will be found useful by some of our readers. We could have used it years ago, and as Mr. Rogers used to say, "It's nice to share."

Sometimes, too much software and too many choices can be a problem. Should we use MTRG, Ethereal, EtherApe, or some other application to monitor network traffic? Should we create logical volumes using linear RAID, LVM, LVM2, or EVMS? Should we do our resumes in TeX, LaTeX, troff, lout, SGML, or XML? You get the idea. If you need to solve a problem but don't know what tool to select from among the myriad choices available, you can spend exponentially more time selecting the right software and ramping up than you do actually solving the problem. For that reason, a book on task-oriented solutions to common problems has been a lot of fun to write, and it should save you many an overnight Google session—as well as providing information that works together and is up to date at the time of writing. All the hacks in this book are techniques that we've used at various times and that we view as time-and hassle-savers that are usually downright fun and cool.

Aside from the "too much software" issue just mentioned, a related concept (and the deep, dark secret of open source) is that not all open source projects are "finished"—ever. (For God's sake, don't tell Microsoft!) Not only do you have many, many choices in the open source space, but the ones you find may do only 95% of what you want, missing on the truly critical 5%. Though there's a lot of really cool-looking, whizzy open source software out there, sometimes the zip gun that reliably fires one bullet using a rubber band is preferable to the chromed fusion-powered death ray that works only 75% of the time—thus books like this one, in which people explain how to accomplish things using packages they've actually used and often still depend on, even if the packages aren't perfect. The tools discussed in these hacks are generally good additions to anyone's toolbox/ library of tips and tricks—and we'll show you how to use them for a variety of purposes.

Again, rather than just explaining how to do specific tasks, we've tried to provide a little background

and context for our approach. This is a book of hacks, but you deserve a little bit of extra info to put the hacks, tools, and solutions in the right context. Where possible, we've also identified other packages and procedures that may accomplish the same goal, but we focus on our preferred solutions for different types of problems.

- [**download The Mormon Tabernacle Choir**](#)
- [**download Growing Herbs Indoors : Your Guide to Growing Herbs in Containers for a Vibrant Indoor Herb Garden**](#)
- [**Every Dead Thing \(Charlie Parker, Book 1\) pdf, azw \(kindle\), .epub**](#)
- [**download online Ellevte Roman, Bok Atten for free**](#)

- <http://junkrobots.com/ebooks/About-Abortion--Ten-Things-a-New-Generation-of-Christians-Should-Know.pdf>
- <http://pittiger.com/lib/Growing-Herbs-Indoors---Your-Guide-to-Growing-Herbs-in-Containers-for-a-Vibrant-Indoor-Herb-Garden.pdf>
- <http://test.markblaustein.com/library/Two-in-the-Bush.pdf>
- <http://test.markblaustein.com/library/Ellevte-Roman--Bok-Atten.pdf>