

EXPERT INSIGHT

---

# Mastering Linux Security and Hardening

A practical guide to protecting your Linux system  
from cyber attacks

**Third Edition**

**<packt>**

**Donald A. Tevault**

# Mastering Linux Security and Hardening

Copyright © 2023 Packt Publishing

All rights reserved. No part of this book may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, without the prior written permission of the publisher, except in the case of brief quotations embedded in critical articles or reviews.

Every effort has been made in the preparation of this book to ensure the accuracy of the information presented. However, the information contained in this book is sold without warranty, either express or implied. Neither the author, nor Packt Publishing, and its dealers and distributors will be held liable for any damages caused or alleged to be caused directly or indirectly by this book.

Packt Publishing has endeavored to provide trademark information about all of the companies and products mentioned in this book by the appropriate use of capitals. However, Packt Publishing cannot guarantee the accuracy of this information.

**Early Access Publication:** Mastering Linux Security and Hardening

**Early Access Production Reference:** B19501

Published by Packt Publishing Ltd.

Livery Place

35 Livery Street

Birmingham

B3 2PB, UK

**ISBN:** 978-1-83763-051-6

[www.packt.com](http://www.packt.com)

[OceanofPDF.com](http://OceanofPDF.com)

# Table of Contents

1. [Mastering Linux Security and Hardening, Third Edition: A practical guide to protecting your Linux system from cyber attacks](#)
2. [1 Running Linux in a Virtual Environment](#)
  - I. [Join our book community on Discord](#)
  - II. [Looking at the threat landscape](#)
  - III. [Why do security breaches happen?](#)
  - IV. [Keeping up with security news](#)
  - V. [Differences between physical, virtual, and cloud setups](#)
  - VI. [Introducing VirtualBox and Cygwin](#)
  - VII. [Installing a virtual machine in VirtualBox](#)
  - VIII. [Installing the EPEL repository on the CentOS 7 virtual machine](#)
  - IX. [Installing the EPEL repository on the AlmaLinux 8/9 virtual machines](#)
  - X. [Configuring a network for VirtualBox virtual machines](#)
  - XI. [Creating a virtual machine snapshot with VirtualBox](#)
  - XII. [Using Cygwin to connect to your virtual machines](#)
  - XIII. [Installing Cygwin on your Windows host](#)
  - XIV. [Using the Windows 10 SSH Client to interface with Linux virtual machines](#)
  - XV. [Using the Windows 11 SSH Client to interface with Linux virtual machines](#)
  - XVI. [Cygwin versus the Windows shell](#)
  - XVII. [Keeping the Linux systems updated](#)
  - XVIII. [Updating Debian-based systems](#)
  - XIX. [Configuring auto updates for Ubuntu](#)
  - XX. [Updating Red Hat 7-based systems](#)
  - XXI. [Updating Red Hat 8/9-based systems](#)
  - XXII. [Managing updates in an enterprise](#)
  - XXIII. [Summary](#)
  - XXIV. [Questions](#)
  - XXV. [Further reading](#)
3. [2 Securing User Accounts](#)
  - I. [Join our book community on Discord](#)

- II. [The dangers of logging in as the root user](#)
- III. [The advantages of using sudo](#)
- IV. [Setting up sudo privileges for full administrative users](#)
  - i. [Adding users to a predefined admin group](#)
  - ii. [Creating an entry in the sudo policy file](#)
- V. [Setting up sudo for users with only certain delegated privileges](#)
  - i. [Hands-on lab for assigning limited sudo privileges](#)
- VI. [Advanced tips and tricks for using sudo](#)
  - i. [The sudo timer](#)
  - ii. [View your sudo privileges](#)
  - iii. [Preventing users from having root shell access](#)
  - iv. [Preventing users from using shell escapes](#)
  - v. [Preventing users from using other dangerous programs](#)
  - vi. [Limiting the user's actions with commands](#)
  - vii. [Letting users run as other users](#)
  - viii. [Preventing abuse via user's shell scripts](#)
  - ix. [Detecting and deleting default user accounts](#)
- VII. [New sudo Features](#)
- VIII. [Special sudo Considerations for SUSE and OpenSUSE](#)
- IX. [Locking down users' home directories the Red Hat way](#)
- X. [Locking down users' home directories the Debian/Ubuntu way](#)
  - i. [useradd on Debian/Ubuntu](#)
  - ii. [adduser on Debian/Ubuntu](#)
- XI. [Enforcing strong password criteria](#)
  - i. [Installing and configuring pwquality](#)
- XII. [Setting and enforcing password and account expiration](#)
- XIII. [Configuring default expiry data for useradd for Red Hat-type systems only](#)
- XIV. [Setting expiry data on a per-account basis with useradd and usermod](#)
- XV. [Setting expiry data on a per-account basis with chage](#)
  - i. [Hands-on lab for setting account and password expiry data](#)
- XVI. [Preventing brute-force password attacks](#)
  - i. [Configuring the pam\\_tally2 PAM module on CentOS 7](#)
  - ii. [Configuring pam\\_faillock on AlmaLinux 8/9](#)
  - iii. [Configuring pam\\_faillock on Ubuntu 20.04 and Ubuntu 22.04](#)

- iv. [Locking user accounts](#)
  - v. [Using usermod to lock a user account](#)
  - vi. [Using passwd to lock user accounts](#)
- XVII. [Locking the root user account](#)
- XVIII. [Setting up security banners](#)
  - i. [Using the motd file](#)
  - ii. [Using the issue file](#)
  - iii. [Using the issue.net file](#)
- XIX. [Detecting compromised passwords](#)
  - i. [Hands-on lab for detecting compromised passwords](#)
- XX. [Understanding centralized user management](#)
  - i. [Microsoft Active Directory](#)
- XXI. [Samba on Linux](#)
  - i. [FreeIPA/Identity Management on RHEL-type distros](#)
- XXII. [Summary](#)
- XXIII. [Questions](#)
- XXIV. [Further reading](#)
- 4. [3 Securing Normal User Accounts](#)
  - I. [Join our book community on Discord](#)
  - II. [Locking down users' home directories the Red Hat way](#)
  - III. [Locking down users' home directories the Debian/Ubuntu way](#)
    - i. [useradd on Debian/Ubuntu](#)
    - ii. [adduser on Debian/Ubuntu](#)
  - IV. [Enforcing strong password criteria](#)
    - i. [Installing and configuring pwquality](#)
  - V. [Setting and enforcing password and account expiration](#)
  - VI. [Configuring default expiry data for useradd for Red Hat-type systems only](#)
  - VII. [Setting expiry data on a per-account basis with useradd and usermod](#)
  - VIII. [Setting expiry data on a per-account basis with chage](#)
    - i. [Hands-on lab for setting account and password expiry data](#)
  - IX. [Preventing brute-force password attacks](#)
    - i. [Configuring the pam\\_tally2 PAM module on CentOS 7](#)
    - ii. [Configuring pam\\_faillock on AlmaLinux 8/9](#)
    - iii. [Configuring pam\\_faillock on Ubuntu 20.04 and Ubuntu 22.04](#)



- iv. [Locking user accounts](#)
  - v. [Using usermod to lock a user account](#)
  - vi. [Using passwd to lock user accounts](#)
- X. [Locking the root user account](#)
- XI. [Setting up security banners](#)
  - i. [Using the motd file](#)
  - ii. [Using the issue file](#)
  - iii. [Using the issue.net file](#)
- XII. [Detecting compromised passwords](#)
  - i. [Hands-on lab for detecting compromised passwords](#)
- XIII. [Understanding centralized user management](#)
  - i. [Microsoft Active Directory](#)
- XIV. [Samba on Linux](#)
  - i. [FreeIPA/Identity Management on RHEL-type distros](#)
- XV. [Summary](#)
- XVI. [Questions](#)
- XVII. [Further Reading](#)
- XVIII. [Answers](#)
- 5. [4 Securing Your Server with a Firewall - Part 1](#)
  - I. [Join our book community on Discord](#)
  - II. [Technical requirements](#)
  - III. [An overview of the Linux firewall](#)
  - IV. [An overview of iptables](#)
    - i. [Mastering the basics of iptables](#)
    - ii. [Blocking ICMP with iptables](#)
    - iii. [Blocking everything that isn't allowed with iptables](#)
    - iv. [Blocking invalid packets with iptables](#)
    - v. [Restoring the deleted rules](#)
    - vi. [Protecting IPv6](#)
  - V. [nftables – a more universal type of firewall system](#)
    - i. [Learning about nftables tables and chains](#)
    - ii. [Configuring nftables on Ubuntu](#)
    - iii. [Using nft commands](#)
  - VI. [Summary](#)
  - VII. [Questions](#)
  - VIII. [Further reading](#)
  - IX. [Answers](#)

## 6. [5 Securing Your Server with a Firewall - Part 2](#)

- I. [Join our book community on Discord](#)
  - II. [Technical requirements](#)
  - III. [Uncomplicated firewall for Ubuntu systems](#)
    - i. [Configuring ufw](#)
    - ii. [Working with the ufw configuration files](#)
  - IV. [firewalld for Red Hat systems](#)
    - i. [Verifying the status of firewalld](#)
    - ii. [Working with firewalld zones](#)
    - iii. [Adding services to a firewalld zone](#)
    - iv. [Adding ports to a firewalld zone](#)
    - v. [Blocking ICMP](#)
    - vi. [Using panic mode](#)
    - vii. [Logging dropped packets](#)
    - viii. [Using firewalld rich language rules](#)
    - ix. [Looking at iptables rules in RHEL/CentOS 7 firewalld](#)
    - x. [Creating direct rules in RHEL/CentOS 7 firewalld](#)
    - xi. [Looking at nftables rules in RHEL/AlmaLinux 8 and 9 firewalld](#)
    - xii. [Creating direct rules in RHEL/AlmaLinux firewalld](#)
  - V. [Summary](#)
  - VI. [Questions](#)
  - VII. [Further reading](#)
  - VIII. [Answers](#)
- ## 7. [6 Encryption Technologies](#)
- I. [Join our book community on Discord](#)
  - II. [GNU Privacy Guard \(GPG\)](#)
    - i. [Hands-on lab – creating your GPG keys](#)
    - ii. [Hands-on lab – symmetrically encrypting your own files](#)
    - iii. [Hands-on lab – encrypting files with public keys](#)
    - iv. [Hands-on lab – signing a file without encryption](#)
  - III. [Encrypting partitions with Linux Unified Key Setup \(LUKS\)](#)
    - i. [Disk encryption during operating system installation](#)
    - ii. [Configuring the LUKS partition to mount automatically](#)
    - iii. [Hands-on lab – configuring the LUKS partition to mount automatically](#)
  - IV. [Encrypting directories with eCryptfs](#)



- i. [Hands-on lab – encrypting a home directory for a new user account](#)
    - ii. [Creating a private directory within an existing home directory](#)
    - iii. [Hands-on lab – encrypting other directories with eCryptfs](#)
  - V. [Encrypting the swap partition with eCryptfs](#)
  - VI. [Using VeraCrypt for cross-platform sharing of encrypted containers](#)
    - i. [Hands-on lab – getting and installing VeraCrypt](#)
    - ii. [Using VeraCrypt in GUI mode](#)
  - VII. [OpenSSL and the public key infrastructure](#)
    - i. [Commercial certificate authorities](#)
    - ii. [Creating keys, certificate signing requests, and certificates](#)
    - iii. [Creating an on-premises CA](#)
    - iv. [Hands-on lab – setting up a Dogtag CA](#)
    - v. [Adding a CA to an operating system](#)
    - vi. [OpenSSL and the Apache web server](#)
    - vii. [Setting up mutual authentication](#)
  - VIII. [Introducing quantum-resistant encryption algorithms](#)
  - IX. [Summary](#)
  - X. [Questions](#)
  - XI. [Further reading](#)
  - XII. [Answers](#)
- 8. [7 SSH Hardening](#)
  - I. [Join our book community on Discord](#)
  - II. [Ensuring that SSH protocol 1 is disabled](#)
  - III. [Creating and managing keys for passwordless logins](#)
    - i. [Creating a user's SSH key set](#)
    - ii. [Transferring the public key to the remote server](#)
    - iii. [Disabling root user login](#)
    - iv. [Disabling username/password logins](#)
    - v. [Enabling two-factor authentication](#)
    - vi. [Configuring Secure Shell with strong encryption algorithms](#)
    - vii. [Scanning for enabled SSH algorithms](#)
    - viii. [Disabling weak SSH encryption algorithms](#)
    - ix. [Setting system-wide encryption policies on RHEL 8/9 and AlmaLinux 8/9](#)

- x. [Configuring more detailed logging](#)
- IV. [Configuring access control with whitelists and TCP Wrappers](#)
  - i. [Configuring whitelists within sshd config](#)
  - ii. [Configuring whitelists with TCP Wrappers](#)
- V. [Configuring automatic logouts and security banners](#)
  - i. [Configuring automatic logout for both local and remote users](#)
  - ii. [Configuring automatic logout in sshd config](#)
  - iii. [Creating a pre-login security banner](#)
- VI. [Configuring other miscellaneous security settings](#)
  - i. [Disabling X11 forwarding](#)
  - ii. [Disabling SSH tunneling](#)
  - iii. [Changing the default SSH port](#)
  - iv. [Managing SSH keys](#)
  - v. [Setting different configurations for different users and groups](#)
  - vi. [Creating different configurations for different hosts](#)
- VII. [Setting up a chroot environment for SFTP users](#)
  - i. [Creating a group and configuring the sshd config file](#)
- VIII. [Sharing a directory with SSHFS](#)
  - i. [Hands-on lab – sharing a directory with SSHFS](#)
- IX. [Remotely connecting from Windows desktops](#)
- X. [Summary](#)
- XI. [Questions](#)
- XII. [Further reading](#)
- XIII. [Answers](#)
- 9. [Section 2: Mastering File and Directory Access Control \(DAC\)](#)
- 10. [8 Mastering Discretionary Access Control](#)
  - I. [Join our book community on Discord](#)
    - i. [Using chown to change ownership of files and directories](#)
    - ii. [Using chmod to set permissions on files and directories](#)
    - iii. [Using SUID and SGID on regular files](#)
    - iv. [The security implications of the SUID and SGID permissions](#)
    - v. [Using extended file attributes to protect sensitive files](#)
    - vi. [Securing system configuration files](#)
  - II. [Summary](#)

- III. [Questions](#)
- IV. [Further reading](#)
- V. [Answers](#)
- 11. [9 Access Control Lists and Shared Directory Management](#)
  - I. [Join our book community on Discord](#)
  - II. [Creating an ACL for either a user or a group](#)
  - III. [Creating an inherited ACL for a directory](#)
  - IV. [Removing a specific permission by using an ACL mask](#)
  - V. [Using the tar --acls option to prevent the loss of ACLs during a backup](#)
  - VI. [Creating a user group and adding members to it](#)
    - i. [Adding members as we create their user accounts](#)
    - ii. [Using usermod to add an existing user to a group](#)
    - iii. [Adding users to a group by editing the /etc/group file](#)
  - VII. [Creating a shared directory](#)
  - VIII. [Setting the SGID bit and the sticky bit on the shared directory](#)
  - IX. [Using ACLs to access files in the shared directory](#)
    - i. [Setting the permissions and creating the ACL](#)
  - X. [Summary](#)
  - XI. [Questions](#)
  - XII. [Further reading](#)
  - XIII. [Answers](#)
- 12. [Section 3: Advanced System Hardening Techniques](#)
- 13. [10 Implementing Mandatory Access Control with SELinux and AppArmor](#)
  - I. [Join our book community on Discord](#)
  - II. [How SELinux can benefit a systems administrator](#)
  - III. [Setting security contexts for files and directories](#)
    - i. [Installing the SELinux tools](#)
    - ii. [Creating web content files with SELinux enabled](#)
    - iii. [Fixing an incorrect SELinux context](#)
  - IV. [Troubleshooting with setroubleshoot](#)
    - i. [Viewing setroubleshoot messages](#)
    - ii. [Using the graphical setroubleshoot utility](#)
    - iii. [Troubleshooting in permissive mode](#)
  - V. [Working with SELinux policies](#)
    - i. [Viewing Booleans](#)

- ii. [Configuring the Booleans](#)
  - iii. [Protecting your web server](#)
  - iv. [Protecting network ports](#)
  - v. [Creating custom policy modules](#)
- VI. [How AppArmor can benefit a systems administrator](#)
  - i. [Looking at AppArmor profiles](#)
  - ii. [Working with AppArmor command-line utilities](#)
  - iii. [Troubleshooting AppArmor problems](#)
  - iv. [Troubleshooting an AppArmor profile – Ubuntu 16.04](#)
  - v. [Troubleshooting an AppArmor profile – Ubuntu 18.04](#)
  - vi. [Troubleshooting Samba problems in Ubuntu 22.04](#)
- VII. [Exploiting a system with an evil Docker container](#)
  - i. [Hands-on lab – Creating an evil Docker container](#)
- VIII. [Summary](#)
- IX. [Questions](#)
- X. [Further reading](#)
- XI. [Answers](#)
- 14. [11 Kernel Hardening and Process Isolation](#)
  - I. [Join our book community on Discord](#)
  - II. [Understanding the /proc filesystem](#)
    - i. [Looking at user-mode processes](#)
    - ii. [Looking at kernel information](#)
  - III. [Setting kernel parameters with sysctl](#)
  - IV. [Configuring the sysctl.conf file](#)
    - i. [Configuring sysctl.conf – Ubuntu](#)
    - ii. [Configuring sysctl.conf – CentOS and AlmaLinux](#)
    - iii. [Setting additional kernel-hardening parameters](#)
    - iv. [Preventing users from seeing each others' processes](#)
  - V. [Understanding process isolation](#)
    - i. [Understanding Control Groups \(cgroups\)](#)
    - ii. [Understanding namespace isolation](#)
    - iii. [Understanding kernel capabilities](#)
    - iv. [Understanding SECCOMP and system calls](#)
    - v. [Using process isolation with Docker containers](#)
    - vi. [Sandboxing with Firejail](#)
    - vii. [Sandboxing with Snappy](#)
    - viii. [Sandboxing with Flatpak](#)

- VI. [Summary](#)
- VII. [Questions](#)
- VIII. [Further reading](#)
- IX. [Answers](#)
- 15. [12 Scanning, Auditing, and Hardening](#)
  - I. [Join our book community on Discord](#)
  - II. [Installing and updating ClamAV and maldet](#)
    - i. [Hands-on lab – installing ClamAV and maldet](#)
    - ii. [Hands-on lab – configuring maldet](#)
    - iii. [Updating ClamAV and maldet](#)
  - III. [Scanning with ClamAV and maldet](#)
    - i. [SELinux considerations](#)
  - IV. [Scanning for rootkits with Rootkit Hunter](#)
    - i. [Hands-on lab – installing and updating Rootkit Hunter](#)
    - ii. [Scanning for rootkits](#)
  - V. [Performing a quick malware analysis with strings and VirusTotal](#)
    - i. [Analyze a file with strings](#)
    - ii. [Scanning the malware with VirusTotal](#)
  - VI. [Understanding the auditd daemon](#)
    - i. [Creating audit rules](#)
    - ii. [Auditing a file for changes](#)
    - iii. [Auditing a directory](#)
    - iv. [Auditing system calls](#)
  - VII. [Using ausearch and aureport](#)
    - i. [Searching for file change alerts](#)
    - ii. [Searching for directory access rule violations](#)
    - iii. [Searching for system call rule violations](#)
    - iv. [Generating authentication reports](#)
    - v. [Using pre-defined rulesets](#)
    - vi. [Hands-on lab – using auditd](#)
    - vii. [Hands-on lab – Using pre-configured rules with auditd](#)
  - VIII. [Auditing files and directories with inotifywait](#)
  - IX. [Applying OpenSCAP policies with oscap](#)
    - i. [Installing OpenSCAP](#)
    - ii. [Viewing the profile files](#)
    - iii. [Getting the missing profiles for Ubuntu](#)
    - iv. [Scanning the system](#)

- v. [Remediating the system](#)
  - vi. [Using SCAP Workbench](#)
  - vii. [Choosing an OpenSCAP profile](#)
  - viii. [Applying an OpenSCAP profile during system installation](#)
- X. [Summary](#)
- XI. [Questions](#)
- XII. [Further reading](#)
- XIII. [Answers](#)
- 16. [13 Logging and Log Security](#)
  - I. [Join our book community on Discord](#)
  - II. [Understanding the Linux system log files](#)
    - i. [The system log and the authentication log](#)
    - ii. [The utmp, wtmp, btmp, and lastlog files](#)
  - III. [Understanding rsyslog](#)
    - i. [Understanding rsyslog logging rules](#)
  - IV. [Understanding journald](#)
  - V. [Making things easier with Logwatch](#)
    - i. [Hands-on lab – installing Logwatch](#)
  - VI. [Setting up a remote log server](#)
    - i. [Hands-on lab – setting up a basic log server](#)
    - ii. [Creating an encrypted connection to the log server](#)
    - iii. [Separating client messages into their own files](#)
  - VII. [Summary](#)
  - VIII. [Questions](#)
  - IX. [Further reading](#)
  - X. [Answers](#)
- 17. [14 Vulnerability Scanning and Intrusion Detection](#)
  - I. [Join our book community on Discord](#)
  - II. [Introduction to Snort and Security Onion](#)
    - i. [Obtaining and installing Snort](#)
  - III. [Using Security Onion](#)
  - IV. [IPFire and its built-in Intrusion Prevention System \(IPS\)](#)
    - i. [Hands-on lab – Creating an IPFire virtual machine](#)
  - V. [Scanning and hardening with Lynis](#)
    - i. [Installing Lynis on Red Hat/CentOS](#)
    - ii. [Installing Lynis on Ubuntu](#)
    - iii. [Scanning with Lynis](#)

- VI. [Finding vulnerabilities with the Greenbone Security Assistant](#)
- VII. [Web server scanning with Nikto](#)
  - i. [Nikto in Kali Linux](#)
- VIII. [Summary](#)
- IX. [Questions](#)
- X. [Further reading](#)
- XI. [Answers](#)
- 18. [15 Prevent Unwanted Programs from Running](#)
  - I. [Join our book community on Discord](#)
  - II. [Mount Partitions with the no options](#)
  - III. [Understanding fapolicyd](#)
    - i. [Understanding the fapolicyd rules](#)
    - ii. [Installing fapolicyd](#)
  - IV. [Summary](#)
  - V. [Further reading](#)
  - VI. [Questions](#)
  - VII. [Answers](#)
- 19. [16 Security Tips and Tricks for the Busy Bee](#)
  - I. [Join our book community on Discord](#)
  - II. [Technical requirements](#)
  - III. [Auditing system services](#)
    - i. [Auditing system services with systemctl](#)
    - ii. [Auditing network services with netstat](#)
    - iii. [Auditing network services with Nmap](#)
  - IV. [Password protecting the GRUB 2 bootloader](#)
    - i. [Hands-on lab – resetting the password for Red Hat/CentOS/AlmaLinux](#)
    - ii. [Hands-on lab – resetting the password for Ubuntu](#)
    - iii. [Preventing kernel parameter edits on Red Hat/CentOS/AlmaLinux](#)
    - iv. [Preventing kernel parameter edits or Recovery mode access on Ubuntu](#)
    - v. [Disabling the submenu for Ubuntu](#)
  - V. [Securely configuring BIOS/UEFI](#)
  - VI. [Using a security checklist for system setup](#)
  - VII. [Summary](#)
  - VIII. [Questions](#)



IX. [Further reading](#)

X. [Answers](#)

[OceanofPDF.com](http://OceanofPDF.com)