- Section 1: Setting up a Secure Linux System
- Running Linux in a Virtual Environment

Looking at the threat landscape
Why do security breaches happen?
Keeping up with security news
Differences between physical, virtual, and cloud setups
Introducing VirtualBox and Cygwin
Installing a virtual machine in VirtualBox
Installing the EPEL repository on the CentOS 7 virtual machine
Installing the EPEL repository on the AlmaLinux 8/9 virtual machines
Configuring a network for VirtualBox virtual machines
Creating a virtual machine snapshot with VirtualBox
Using Cygwin to connect to your virtual machines
Installing Cygwin on your Windows host
Using the Windows 10 SSH client to interface with Linux virtual machines
Using the Windows 11 SSH client to interface with Linux virtual machines
Cygwin versus the Windows shell
Keeping the Linux systems updated
Updating Debian-based systems
Configuring auto updates for Ubuntu
Updating Red Hat 7-based systems
Updating Red Hat 8/9-based systems
Managing updates in an enterprise
Summary
Questions
Further reading
Answers

- Securing Administrative User Accounts

The dangers of logging in as the root user
The advantages of using sudo
Setting up sudo privileges for full administrative users
Adding users to a predefined admin group
Creating an entry in the sudo policy file
Setting up sudo for users with only certain delegated privileges
Hands-on lab for assigning limited sudo privileges
Advanced tips and tricks for using sudo
The sudo timer
View your sudo privileges
Hands-on lab for disabling the sudo timer
Preventing users from having root shell access
Preventing users from using shell escapes
Preventing users from using other dangerous programs
Limiting the user's actions with commands
Letting users run as other users
Preventing abuse via a user's shell scripts
Detecting and deleting default user accounts

New sudo features
Special sudo considerations for SUSE and OpenSUSE
Summary
Questions
Further reading
Answers
 Securing Normal User Accounts
Locking down users' home directories the Red Hat way
Locking down users' home directories the Debian/Ubuntu way
useradd on Debian/Ubuntu
adduser on Debian/Ubuntu
Hands-on lab for creating an encrypted home directory with adduser
Enforcing strong password criteria
Installing and configuring pwquality
Hands-on lab for setting password complexity criteria
Setting and enforcing password and account expiration
Configuring default expiry data for useradd for Red Hat-type systems only
Setting expiry data on a per-account basis with useradd and usermod
Setting expiry data on a per-account basis with chage
Hands-on lab for setting account and password expiry data
Preventing brute-force password attacks
Configuring the pam_tally2 PAM module on CentOS 7
Hands-on lab for configuring pam_tally2 on CentOS 7
Configuring pam_faillock on AlmaLinux 8/9
Hands-on lab for configuring pam_faillock on AlmaLinux 8 or AlmaLinux 9
Configuring pam_faillock on Ubuntu 20.04 and Ubuntu 22.04
Hands-on lab for configuring pam_faillock on Ubuntu 20.04 and Ubuntu 22.04
Locking user accounts
Using usermod to lock a user account
Using passwd to lock user accounts
Locking the root user account
Setting up security banners
Using the motd file
Using the issue file
Using the issue.net file
Detecting compromised passwords
Hands-on lab for detecting compromised passwords
Understanding centralized user management
Microsoft Active Directory
Samba on Linux
FreeIPA/Identity Management on RHEL-type distros
Summary
Questions
Further reading
Answers
 Securing Your Server with a Firewall – Part 1

Technical requirements
An overview of the Linux firewall
An overview of iptables
Mastering the basics of iptables
Blocking ICMP with iptables
Blocking everything that isn’t allowed with iptables
Hands-on lab for basic iptables usage
Blocking invalid packets with iptables
Restoring the deleted rules
Hands-on lab for blocking invalid IPv4 packets
Protecting IPv6
Hands-on lab for ip6tables
nftables – a more universal type of firewall system
Learning about nftables tables and chains
Getting started with nftables
Configuring nftables on Ubuntu
Using nft commands
Hands-on lab for nftables on Ubuntu
Summary
Questions
Further reading
Answers
 Securing Your Server with a Firewall — Part 2
Technical requirements
The Uncomplicated Firewall for Ubuntu systems
Configuring ufw
Working with the ufw configuration files
Hands-on lab for basic ufw usage
firewalld for Red Hat systems
Verifying the status of firewalld
Working with firewalld zones
Adding services to a firewalld zone
Adding ports to a firewalld zone
Blocking ICMP
Using panic mode
Logging dropped packets
Using firewalld rich language rules
Looking at iptables rules in RHEL/CentOS 7 firewalld
Creating direct rules in RHEL/CentOS 7 firewalld
Looking at nftables rules in RHEL/AlmaLinux 8 and 9 firewalld
Creating direct rules in RHEL/AlmaLinux firewalld
Hands-on lab for firewalld commands
Summary
Questions
Further reading
Answers

- Encryption Technologies
GNU Privacy Guard (GPG)
Hands-on lab – creating your GPG keys
Hands-on lab – symmetrically encrypting your own files
Hands-on lab – encrypting files with public keys
Hands-on lab – signing a file without encryption
Encrypting partitions with Linux Unified Key Setup (LUKS)
Disk encryption during operating system installation
Hands-on lab – adding an encrypted partition with LUKS
Configuring the LUKS partition to mount automatically
Hands-on lab – configuring the LUKS partition to mount automatically
Encrypting directories with eCryptfs
Hands-on lab – encrypting a home directory for a new user account
Creating a private directory within an existing home directory
Hands-on lab – encrypting other directories with eCryptfs
Encrypting the swap partition with eCryptfs
Using VeraCrypt for cross-platform sharing of encrypted containers
Hands-on lab – getting and installing VeraCrypt
Hands-on lab – creating and mounting a VeraCrypt volume in console mode
Using VeraCrypt in GUI mode
OpenSSL and the Public Key Infrastructure
Commercial certificate authorities
Creating keys, certificate signing requests, and certificates
Creating a self-signed certificate with an RSA key
Creating a self-signed certificate with an Elliptic Curve key
Creating an RSA key and a Certificate Signing Request
Creating an EC key and a CSR
Creating an on-premises CA
Hands-on lab – setting up a Dogtag CA
Adding a CA to an operating system
Hands-on lab – exporting and importing the Dogtag CA certificate
Importing the CA into Windows
OpenSSL and the Apache webserver
Hardening Apache SSL/TLS on Ubuntu
Hardening Apache SSL/TLS on RHEL 9/AlmaLinux 9
Setting FIPS mode on RHEL 9/AlmaLinux 9
Hardening Apache SSL/TLS on RHEL 7/CentOS 7
Setting up mutual authentication
Introducing quantum-resistant encryption algorithms
Summary
Questions
Further reading
Answers
- SSH Hardening
Ensuring that SSH protocol 1 is disabled
Creating and managing keys for passwordless logins

Creating a user's SSH key set
Transferring the public key to the remote server
Hands-on lab – creating and transferring SSH keys
Disabling root user login
Disabling username/password logins
Hands-on lab – Disabling root login and password authentication
Enabling two-factor authentication
Hands-on lab — Setting up two-factor authentication on Ubuntu 22.04
Hands-on lab – Using Google Authenticator with key exchange on Ubuntu
Hands-on lab — Setting up two-factor authentication on AlmaLinux 8
Hand-on lab — Using Google Authenticator with key exchange on AlmaLinux 8
Configuring Secure Shell with strong encryption algorithms
Understanding SSH encryption algorithms
Scanning for enabled SSH algorithms
Hands-on lab – Scanning with Nmap
Disabling weak SSH encryption algorithms
Hands-on lab – disabling weak SSH encryption algorithms – Ubuntu 22.04
Hands-on lab – disabling weak SSH encryption algorithms – CentOS 7
Setting system-wide encryption policies on RHEL 8/9 and AlmaLinux 8/9
Hands-on lab – setting encryption policies on AlmaLinux 9
Configuring more detailed logging
Hands-on lab – configuring more verbose SSH logging
Configuring access control with whitelists and TCP Wrappers
Configuring whitelists within sshd_config
Hands-on lab – configuring whitelists within sshd_config
Configuring whitelists with TCP Wrappers
Configuring automatic logouts and security banners
Configuring automatic logout for both local and remote users
Configuring automatic logout in sshd_config
Creating a pre-login security banner
Configuring other miscellaneous security settings
Disabling X11 forwarding
Disabling SSH tunneling
Changing the default SSH port
Managing SSH keys
Setting different configurations for different users and groups
Creating different configurations for different hosts
Setting up a chroot environment for SFTP users
Creating a group and configuring the sshd_config file
Hands-on lab – Setting up a chroot directory for the sftpusers group
Sharing a directory with SSHFS
Hands-on lab – Sharing a directory with SSHFS
Remotely connecting from Windows desktops
Summary
Questions
Further reading

Answers
 Section 2: Mastering File and Directory Access Control (DAC)
 Mastering Discretionary Access Control
Using chown to change ownership of files and directories
Using chmod to set permissions on files and directories
Setting permissions with the symbolic method
Setting permissions with the numerical method
Using SUID and SGID on regular files
The security implications of the SUID and SGID permissions
Finding spurious SUID or SGID files
Preventing SUID and SGID usage on a partition
Using extended file attributes to protect sensitive files
Setting the a attribute
Setting the i attribute
Securing system configuration files
Summary
Questions
Further reading
Answers
 Access Control Lists and Shared Directory Management
Creating an ACL for either a user or a group
Creating an inherited ACL for a directory
Removing a specific permission by using an ACL mask
Using the tar --acls option to prevent the loss of ACLs during a backup
Creating a user group and adding members to it
Adding members as we create their user accounts
Using usermod to add an existing user to a group
Adding users to a group by editing the /etc/group file
Creating a shared directory
Setting the SGID bit and the sticky bit on the shared directory
Using ACLs to access files in the shared directory
Setting the permissions and creating the ACL
Hands-on lab – creating a shared group directory
Summary
Questions
Further reading
Answers
 Section 3: Advanced System Hardening Techniques
 Implementing Mandatory Access Control with SELinux and AppArmor
How SELinux can benefit a systems administrator
Setting security contexts for files and directories
Installing the SELinux tools
Creating web content files with SELinux enabled
Fixing an incorrect SELinux context
Using chcon
Using restorecon

Using semanage
Hands-on lab – SELinux type enforcement
Troubleshooting with setroubleshoot
Viewing setroubleshoot messages
Using the graphical setroubleshoot utility
Troubleshooting in permissive mode
Working with SELinux policies
Viewing Booleans
Configuring the Booleans
Protecting your web server
Protecting network ports
Creating custom policy modules
Hands-on lab – SELinux Booleans and ports
How AppArmor can benefit a systems administrator
Looking at AppArmor profiles
Working with AppArmor command-line utilities
Troubleshooting AppArmor problems
Troubleshooting an AppArmor profile – Ubuntu 16.04
Troubleshooting an AppArmor profile – Ubuntu 18.04
Hands-on lab – Troubleshooting an AppArmor profile
Troubleshooting Samba problems in Ubuntu 22.04
Exploiting a system with an evil Docker container
Hands-on lab – Creating an evil Docker container
Summary
Questions
Further reading
Answers
 Kernel Hardening and Process Isolation
Understanding the /proc filesystem
Looking at user-mode processes
Looking at kernel information
Setting kernel parameters with sysctl
Configuring the sysctl.conf file
Configuring sysctl.conf – Ubuntu
Configuring sysctl.conf – CentOS and AlmaLinux
Setting additional kernel-hardening parameters
Hands-on lab – scanning kernel parameters with Lynis
Preventing users from seeing each others' processes
Understanding process isolation
Understanding Control Groups (cgroups)
Understanding namespace isolation
Understanding kernel capabilities
Hands-on lab – setting a kernel capability
Understanding SECCOMP and system calls
Using process isolation with Docker containers
Sandboxing with Firejail

Hands-on lab – using Firejail
Sandboxing with Snappy
Sandboxing with Flatpak
Summary
Questions
Further reading
Answers
 Scanning, Auditing, and Hardening
Installing and updating ClamAV and maldet
Hands-on lab – installing ClamAV and maldet
Hands-on lab – configuring maldet
Updating ClamAV and maldet
Scanning with ClamAV and maldet
SELinux considerations
Scanning for rootkits with Rootkit Hunter
Hands-on lab – installing and updating Rootkit Hunter
Scanning for rootkits
Performing a quick malware analysis with strings and VirusTotal
Analyze a file with strings
Scanning the malware with VirusTotal
Understanding the auditd daemon
Creating audit rules
Auditing a file for changes
Auditing a directory
Auditing system calls
Using ausearch and aureport
Searching for file change alerts
Searching for directory access rule violations
Searching for system call rule violations
Generating authentication reports
Using pre-defined rulesets
Hands-on lab – using auditd
Hands-on lab –Using pre-configured rules with auditd
Auditing files and directories with inotifywait
Applying OpenSCAP policies with oscap
Installing OpenSCAP
Viewing the profile files
Getting the missing profiles for Ubuntu
Scanning the system
Remediating the system
Using SCAP Workbench
Choosing an OpenSCAP profile
Applying an OpenSCAP profile during system installation
Summary
Questions
Further reading

Answers
 Logging and Log Security
Understanding the Linux system log files
The system log and the authentication log
The utmp, wtmp, btmp, and lastlog files
Understanding rsyslog
Understanding rsyslog logging rules
Understanding journald
Making things easier with Logwatch
Hands-on lab – installing Logwatch
Setting up a remote log server
Hands-on lab – setting up a basic log server
Creating an encrypted connection to the log server
Creating a stunnel connection on AlmaLinux 9 – server side
Creating a stunnel connection on AlmaLinux – client side
Creating a stunnel connection on Ubuntu – server side
Creating a stunnel connection on Ubuntu – client side
Separating client messages into their own files
Maintaining Logs in Large Enterprises
Summary
Questions
Further reading
Answers
 Vulnerability Scanning and Intrusion Detection
Introduction to Snort and Security Onion
Obtaining and installing Snort
Hands-on lab – installing Snort via a Docker container
Using Security Onion
IPFire and its built-in Intrusion Prevention System (IPS)
Hands-on lab – Creating an IPFire virtual machine
Scanning and hardening with Lynis
Installing Lynis on Red Hat/CentOS
Installing Lynis on Ubuntu
Scanning with Lynis
Finding vulnerabilities with the Greenbone Security Assistant
Web server scanning with Nikto
Nikto in Kali Linux
Hands-on lab–Installing Nikto from Github
Scanning a web server with Nikto
Summary
Questions
Further reading
Answers
 Prevent Unwanted Programs from Running
Mount Partitions with the no options
Understanding fapolicyd

Understanding the fapolicyd rules
Installing fapolicyd
Summary
Further reading
Questions
Answers
 Security Tips and Tricks for the Busy Bee
Technical requirements
Auditing system services
Auditing system services with systemctl
Auditing network services with netstat
Hands-on lab – viewing network services with netstat
Auditing network services with Nmap
Port states
Scan types
Hands-on lab – scanning with Nmap
Password-protecting the GRUB2 bootloader
Hands-on lab – resetting the password for Red Hat/CentOS/AlmaLinux
Hands-on lab – resetting the password for Ubuntu
Preventing kernel parameter edits on Red Hat/CentOS/AlmaLinux
Preventing kernel parameter edits or recovery mode access on Ubuntu
Disabling the submenu for Ubuntu
Securely configuring BIOS/UEFI
Using a security checklist for system setup
Summary
Questions
Further reading
Answers
 Other Books You May Enjoy
 Index