

Security Strategies In Linux Platforms And Applications Jones Bartlett Learning Information Systems Security Assurance

Penetration testers simulate cyber attacks to find security weaknesses in networks, operating systems, and applications. Information security experts worldwide use penetration techniques to evaluate enterprise defenses. In *Penetration Testing*, security expert, researcher, and trainer Georgia Weidman introduces you to the core skills and techniques that every pentester needs. Using a virtual machine–based lab that includes Kali Linux and vulnerable operating systems, you'll run through a series of practical lessons with tools like Wireshark, Nmap, and Burp Suite. As you follow along with the labs and launch attacks, you'll experience the key stages of an actual assessment—including information gathering, finding exploitable vulnerabilities, gaining access to systems, post exploitation, and more. Learn how to:

- Crack passwords and wireless network keys with brute-forcing and wordlists
- Test web applications for vulnerabilities
- Use the Metasploit Framework to launch exploits and write your own Metasploit modules
- Automate social-engineering attacks
- Bypass antivirus software
- Turn access to one machine into total control of the enterprise in the post exploitation phase

You'll even explore writing your own exploits. Then it's on to mobile hacking—Weidman's particular area of research—with her tool, the Smartphone Pentest Framework. With its collection of hands-on lessons that cover key tools and strategies, *Penetration Testing* is the introduction that every aspiring hacker needs.

PART OF THE NEW JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES! *Security Strategies in Linux Platforms and Applications* covers every major aspect of security on a Linux system. Written by an industry expert, this book is divided into three natural parts to illustrate key concepts in the field. It opens with a discussion on the risks, threats, and vulnerabilities associated with Linux as an operating system using examples from Red Hat Enterprise Linux and Ubuntu. Part 2 discusses how to take advantage of the layers of security available to Linux—user and group options, filesystems, and security options for important services, as well as the security modules associated with AppArmor and SELinux. The book closes with a look at the use of both open source and proprietary tools when building a layered security strategy for Linux operating system environments. Using real-world examples and exercises, this useful resource incorporates hands-on activities to walk students through the fundamentals of security strategies related to the Linux system.

This practical, tutorial-style book uses the Kali Linux distribution to teach Linux basics with a focus on how hackers would use them. Topics include Linux command line basics, filesystems, networking, BASH basics, package management, logging, and the Linux kernel and drivers. If you're getting started along the exciting path of hacking, cybersecurity, and pentesting, *Linux Basics for Hackers* is an excellent first step. Using Kali Linux, an advanced penetration testing distribution of Linux, you'll learn the basics of using the Linux operating system and acquire the tools and techniques you'll need to take control of a Linux environment. First, you'll learn how to install Kali on a virtual machine and get an introduction to basic Linux concepts. Next, you'll tackle broader Linux topics like manipulating text, controlling file and directory permissions, and managing user environment variables. You'll then focus in on foundational hacking concepts like security and anonymity and learn scripting skills with bash and Python. Practical tutorials and exercises throughout will reinforce and test your skills as you learn how to:

- Cover your tracks by changing your network information and manipulating the rsyslog logging utility
- Write a tool to scan for network connections, and connect and listen to wireless

Read Book Security Strategies In Linux Platforms And Applications Jones Bartlett Learning Information Systems Security Assurance

networks - Keep your internet activity stealthy using Tor, proxy servers, VPNs, and encrypted email - Write a bash script to scan open ports for potential targets - Use and abuse services like MySQL, Apache web server, and OpenSSH - Build your own hacking tools, such as a remote video spy camera and a password cracker Hacking is complex, and there is no single way in. Why not start at the beginning with Linux Basics for Hackers?

"This book covers strategies on using and evaluating open source products for online teaching and learning systems"--Provided by publisher.

Over 120 recipes to perform advanced penetration testing with Kali Linux About This Book Practical recipes to conduct effective penetration testing using the powerful Kali Linux Leverage tools like Metasploit, Wireshark, Nmap, and many more to detect vulnerabilities with ease Confidently perform networking and application attacks using task-oriented recipes Who This Book Is For This book is aimed at IT security professionals, pentesters, and security analysts who have basic knowledge of Kali Linux and want to conduct advanced penetration testing techniques. What You Will Learn Installing, setting up and customizing Kali for pentesting on multiple platforms Pentesting routers and embedded devices Bug hunting 2017 Pwning and escalating through corporate network Buffer overflows 101 Auditing wireless networks Fiddling around with software-defined radio Hacking on the run with NetHunter Writing good quality reports In Detail With the current rate of hacking, it is very important to pentest your environment in order to ensure advanced-level security. This book is packed with practical recipes that will quickly get you started with Kali Linux (version 2016.2) according to your needs, and move on to core functionalities. This book will start with the installation and configuration of Kali Linux so that you can perform your tests. You will learn how to plan attack strategies and perform web application exploitation using tools such as Burp, and Jexboss. You will also learn how to perform network exploitation using Metasploit, Sparta, and Wireshark. Next, you will perform wireless and password attacks using tools such as Patator, John the Ripper, and airoscript-ng. Lastly, you will learn how to create an optimum quality pentest report! By the end of this book, you will know how to conduct advanced penetration testing thanks to the book's crisp and task-oriented recipes. Style and approach This is a recipe-based book that allows you to venture into some of the most cutting-edge practices and techniques to perform penetration testing with Kali Linux.

Hacking with Kali introduces you the most current distribution of the de facto standard tool for Linux pen testing. Starting with use of the Kali live CD and progressing through installation on hard drives, thumb drives and SD cards, author James Broad walks you through creating a custom version of the Kali live distribution. You'll learn how to configure networking components, storage devices and system services such as DHCP and web services. Once you're familiar with the basic components of the software, you'll learn how to use Kali through the phases of the penetration testing lifecycle; one major tool from each phase is explained. The book culminates with a chapter on reporting that will provide examples of documents used prior to, during and after the pen test. This guide will benefit information security professionals of all levels, hackers, systems administrators, network administrators, and beginning and intermediate professional pen testers, as well as students majoring in information security. Provides detailed explanations of the complete penetration testing lifecycle Complete linkage of the Kali information, resources and distribution downloads Hands-on exercises reinforce topics

The Laboratory Manual Version 1.5 To Accompany Security Strategies In Linux Platforms And Applications Is The Lab Companion To The Information Systems And Security Series Title, Security Strategies In Linux Platforms And Applications. It Provides Hands-On Exercises Using The Jones & Bartlett Learning Virtual Security Cloud Labs, That Provide Real-World Experience With Measurable Learning Outcomes. About The Series: Visit www.issaseries.com For A Complete Look At The Series! The Jones & Bartlett Learning

Read Book Security Strategies In Linux Platforms And Applications Jones Bartlett Learning Information Systems Security Assurance

Information System & Assurance Series Delivers Fundamental IT Security Principles Packed With Real-World Applications And Examples For IT Security, Cybersecurity, Information Assurance, And Information Systems Security Programs. Authored By Certified Information Systems Security Professionals (Cissps), And Reviewed By Leading Technical Experts In The Field, These Books Are Current Forward-Thinking Resources That Enable Readers To Solve The Cybersecurity Challenges Of Today And Tomorrow.

Achieve the gold standard in penetration testing with Kali using this masterpiece, now in its third edition! About This Book Get a rock-solid insight into penetration testing techniques and test your corporate network against threats like never before Formulate your pentesting strategies by relying on the most up-to-date and feature-rich Kali version in town—Kali Linux 2 (aka Sana). Experience this journey with new cutting-edge wireless penetration tools and a variety of new features to make your pentesting experience smoother Who This Book Is For If you are an IT security professional or a student with basic knowledge of Unix/Linux operating systems, including an awareness of information security factors, and you want to use Kali Linux for penetration testing, this book is for you. What You Will Learn Find out to download and install your own copy of Kali Linux Properly scope and conduct the initial stages of a penetration test Conduct reconnaissance and enumeration of target networks Exploit and gain a foothold on a target system or network Obtain and crack passwords Use the Kali Linux NetHunter install to conduct wireless penetration testing Create proper penetration testing reports In Detail Kali Linux is a comprehensive penetration testing platform with advanced tools to identify, detect, and exploit the vulnerabilities uncovered in the target network environment. With Kali Linux, you can apply appropriate testing methodology with defined business objectives and a scheduled test plan, resulting in a successful penetration testing project engagement. Kali Linux – Assuring Security by Penetration Testing is a fully focused, structured book providing guidance on developing practical penetration testing skills by demonstrating cutting-edge hacker tools and techniques with a coherent, step-by-step approach. This book offers you all of the essential lab preparation and testing procedures that reflect real-world attack scenarios from a business perspective, in today's digital age. Style and approach This practical guide will showcase penetration testing through cutting-edge tools and techniques using a coherent, step-by-step approach.

Written as an interactive tutorial, this book covers the core of Kali Linux with real-world examples and step-by-step instructions to provide professional guidelines and recommendations for you. The book is designed in a simple and intuitive manner that allows you to explore the whole Kali Linux testing process or study parts of it individually. If you are an IT security professional who has a basic knowledge of Unix/Linux operating systems, including an awareness of information security factors, and want to use Kali Linux for penetration testing, then this book is for you.

Security Strategies in Linux Platforms and Applications Jones & Bartlett Publishers

PART OF THE NEW JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES! More than 90 percent of individuals, students, educators, businesses, organizations, and governments use Microsoft Windows, which has experienced frequent attacks against its well-publicized vulnerabilities. Written by an industry expert, Security Strategies in Windows Platforms and Applications focuses on new risks, threats, and

vulnerabilities associated with the Microsoft Windows operating system. Particular emphasis is placed on Windows XP, Vista, and 7 on the desktop, and Windows Server 2003 and 2008 versions. It highlights how to use tools and techniques to decrease risks arising from vulnerabilities in Microsoft Windows operating systems and applications. The book also includes a resource for readers desiring more information on Microsoft Windows OS hardening, application security, and incident management. With its accessible writing style, and step-by-step examples, this must-have resource will ensure readers are educated on the latest Windows security strategies and techniques.

Build a resilient network and prevent advanced cyber attacks and breaches Key Features Explore modern cybersecurity techniques to protect your networks from ever-evolving cyber threats Prevent cyber attacks by using robust cybersecurity strategies Unlock the secrets of network security Book Description With advanced cyber attacks severely impacting industry giants and the constantly evolving threat landscape, organizations are adopting complex systems to maintain robust and secure environments. Network Security Strategies will help you get well-versed with the tools and techniques required to protect any network environment against modern cyber threats. You'll understand how to identify security vulnerabilities across the network and how to effectively use a variety of network security techniques and platforms. Next, the book will show you how to design a robust network that provides top-notch security to protect against traditional and new evolving attacks. With the help of detailed solutions and explanations, you'll be able to monitor networks skillfully and identify potential risks. Finally, the book will cover topics relating to thought leadership and the management aspects of network security. By the end of this network security book, you'll be well-versed in defending your network from threats and be able to consistently maintain operational efficiency, security, and privacy in your environment. What you will learn Understand network security essentials, including concepts, mechanisms, and solutions to implement secure networks Get to grips with setting up and threat monitoring cloud and wireless networks Defend your network against emerging cyber threats in 2020 Discover tools, frameworks, and best practices for network penetration testing Understand digital forensics to enhance your network security skills Adopt a proactive approach to stay ahead in network security Who this book is for This book is for anyone looking to explore information security, privacy, malware, and cyber threats. Security experts who want to enhance their skill set will also find this book useful. A prior understanding of cyber threats and information security will help you understand the key concepts covered in the book more effectively.

Discover how poor identity and privilege management can be leveraged to compromise accounts and credentials within an organization. Learn how role-based identity assignments, entitlements, and auditing strategies can be implemented to mitigate the threats leveraging accounts and identities and how to manage compliance for regulatory initiatives. As a solution, Identity Access

Management (IAM) has emerged as the cornerstone of enterprise security. Managing accounts, credentials, roles, certification, and attestation reporting for all resources is now a security and compliance mandate. When identity theft and poor identity management is leveraged as an attack vector, risk and vulnerabilities increase exponentially. As cyber attacks continue to increase in volume and sophistication, it is not a matter of if, but when, your organization will have an incident. Threat actors target accounts, users, and their associated identities, to conduct their malicious activities through privileged attacks and asset vulnerabilities. Identity Attack Vectors details the risks associated with poor identity management practices, the techniques that threat actors and insiders leverage, and the operational best practices that organizations should adopt to protect against identity theft and account compromises, and to develop an effective identity governance program. What You Will Learn Understand the concepts behind an identity and how their associated credentials and accounts can be leveraged as an attack vector Implement an effective Identity Access Management (IAM) program to manage identities and roles, and provide certification for regulatory compliance See where identity management controls play a part of the cyber kill chain and how privileges should be managed as a potential weak link Build upon industry standards to integrate key identity management technologies into a corporate ecosystem Plan for a successful deployment, implementation scope, measurable risk reduction, auditing and discovery, regulatory reporting, and oversight based on real-world strategies to prevent identity attack vectors Who This Book Is For Management and implementers in IT operations, security, and auditing looking to understand and implement an identity access management program and manage privileges in these environments

Ten Strategies of a World-Class Cyber Security Operations Center conveys MITRE's accumulated expertise on enterprise-grade computer network defense. It covers ten key qualities of leading Cyber Security Operations Centers (CSOCs), ranging from their structure and organization, to processes that best enable smooth operations, to approaches that extract maximum value from key CSOC technology investments. This book offers perspective and context for key decision points in structuring a CSOC, such as what capabilities to offer, how to architect large-scale data collection and analysis, and how to prepare the CSOC team for agile, threat-based response. If you manage, work in, or are standing up a CSOC, this book is for you. It is also available on MITRE's website, www.mitre.org.

PART OF THE NEW JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES! Security Strategies in Linux Platforms and Applications covers every major aspect of security on a Linux system. Written by an industry expert, this book is divided into three natural parts to illustrate key concepts in the field. It opens with a discussion on the risks, threats, and vulnerabilities associated with Linux as an operating system using

examples from Red Hat Enterprise Linux and Ubuntu. Part 2 discusses how to take advantage of the layers of security available to Linux--user and group options, filesystems, and security options for important services, as well as the security modules associated with AppArmor and SELinux. The book closes with a look at the use of both open source and proprietary tools when building a layered security strategy for Linux operating system environments. Using real-world examples and exercises, this useful resource incorporates hands-on activities to walk students through the fundamentals of security strategies related to the Linux system.

The Second Edition of Security Strategies in Linux Platforms and Applications covers every major aspect of security on a Linux system. Written by an industry expert, this book is divided into three natural parts to illustrate key concepts in the field. It opens with a discussion of the risks, threats, and vulnerabilities associated with Linux as an operating system using current examples and cases. Part 2 discusses how to take advantage of the layers of security available to Linux--user and group options, filesystems, and security options for important services, as well as the security modules associated with AppArmor and SELinux. The book closes with a look at the use of both open source and proprietary tools when building a layered security strategy for Linux operating system environments. Using real-world examples and exercises, this useful resource incorporates hands-on activities to walk readers through the fundamentals of security strategies related to the Linux system.

Kali Linux Network Scanning Cookbook is intended for information security professionals and casual security enthusiasts alike. It will provide the foundational principles for the novice reader but will also introduce scripting techniques and in-depth analysis for the more advanced audience. Whether you are brand new to Kali Linux or a seasoned veteran, this book will aid in both understanding and ultimately mastering many of the most powerful and useful scanning techniques in the industry. It is assumed that the reader has some basic security testing experience.

See how privileges, insecure passwords, administrative rights, and remote access can be combined as an attack vector to breach any organization. Cyber attacks continue to increase in volume and sophistication. It is not a matter of if, but when, your organization will be breached. Threat actors target the path of least resistance: users and their privileges. In decades past, an entire enterprise might be sufficiently managed through just a handful of credentials. Today's environmental complexity has seen an explosion of privileged credentials for many different account types such as domain and local administrators, operating systems (Windows, Unix, Linux, macOS, etc.), directory services, databases, applications, cloud instances, networking hardware, Internet of Things (IoT), social media, and so many more. When unmanaged, these privileged credentials pose a significant threat from external hackers and insider threats. We are experiencing an expanding universe of privileged accounts almost everywhere.

There is no one solution or strategy to provide the protection you need against all vectors and stages of an attack. And while some new and innovative products will help protect against or detect against a privilege attack, they are not guaranteed to stop 100% of malicious activity. The volume and frequency of privilege-based attacks continues to increase and test the limits of existing security controls and solution implementations. Privileged Attack Vectors details the risks associated with poor privilege management, the techniques that threat actors leverage, and the defensive measures that organizations should adopt to protect against an incident, protect against lateral movement, and improve the ability to detect malicious activity due to the inappropriate usage of privileged credentials. This revised and expanded second edition covers new attack vectors, has updated definitions for privileged access management (PAM), new strategies for defense, tested empirical steps for a successful implementation, and includes new disciplines for least privilege endpoint management and privileged remote access. What You Will Learn Know how identities, accounts, credentials, passwords, and exploits can be leveraged to escalate privileges during an attack Implement defensive and monitoring strategies to mitigate privilege threats and risk Understand a 10-step universal privilege management implementation plan to guide you through a successful privilege access management journey Develop a comprehensive model for documenting risk, compliance, and reporting based on privilege session activity Who This Book Is For Security management professionals, new security professionals, and auditors looking to understand and solve privilege access management problems "This book offers comprehensive explanations of topics in computer system security in order to combat the growing risk associated with technology"--Provided by publisher.

PART OF THE NEW JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES Fully revised and updated with the latest data from the field, Network Security, Firewalls, and VPNs, Second Edition provides a unique, in-depth look at the major business challenges and threats that are introduced when an organization's network is connected to the public Internet. Written by an industry expert, this book provides a comprehensive explanation of network security basics, including how hackers access online networks and the use of Firewalls and VPNs to provide security countermeasures. Using examples and exercises, this book incorporates hands-on activities to prepare the reader to disarm threats and prepare for emerging technologies and future attacks. Key Features: -Introduces the basics of network security exploring the details of firewall security and how VPNs operate -Illustrates how to plan proper network security to combat hackers and outside threats -Discusses firewall configuration and deployment and managing firewall security -Identifies how to secure local and internet communications with a VPN Instructor Materials for Network Security, Firewalls, VPNs include: PowerPoint Lecture Slides Exam Questions Case Scenarios/Handouts About the Series This

book is part of the Information Systems Security and Assurance Series from Jones and Bartlett Learning. Designed for courses and curriculums in IT Security, Cybersecurity, Information Assurance, and Information Systems Security, this series features a comprehensive, consistent treatment of the most current thinking and trends in this critical subject area. These titles deliver fundamental information-security principles packed with real-world applications and examples. Authored by Certified Information Systems Security Professionals (CISSPs), they deliver comprehensive information on all aspects of information security.

Reviewed word for word by leading technical experts in the field, these books are not just current, but forward-thinking putting you in the position to solve the cybersecurity challenges not just of today, but of tomorrow, as well."

ALL YOU NEED TO KNOW TO SECURE LINUX SYSTEMS, NETWORKS, APPLICATIONS, AND DATA—IN ONE BOOK From the basics to advanced techniques: no Linux security experience necessary Realistic examples & step-by-step activities: practice hands-on without costly equipment The perfect introduction to Linux-based security for all students and IT professionals Linux distributions are widely used to support mission-critical applications and manage crucial data. But safeguarding modern Linux systems is complex, and many Linux books have inadequate or outdated security coverage. Linux Essentials for Cybersecurity is your complete solution. Leading Linux certification and security experts William "Bo" Rothwell and Dr. Denise Kinsey introduce Linux with the primary goal of enforcing and troubleshooting security. Their practical approach will help you protect systems, even if one or more layers are penetrated. First, you'll learn how to install Linux to achieve optimal security upfront, even if you have no Linux experience. Next, you'll master best practices for securely administering accounts, devices, services, processes, data, and networks. Then, you'll master powerful tools and automated scripting techniques for footprinting, penetration testing, threat detection, logging, auditing, software management, and more. To help you earn certification and demonstrate skills, this guide covers many key topics on CompTIA Linux+ and LPIC-1 exams. Everything is organized clearly and logically for easy understanding, effective classroom use, and rapid on-the-job training. **LEARN HOW TO:** Review Linux operating system components from the standpoint of security Master key commands, tools, and skills for securing Linux systems Troubleshoot common Linux security problems, one step at a time Protect user and group accounts with Pluggable Authentication Modules (PAM), SELinux, passwords, and policies Safeguard files and directories with permissions and attributes Create, manage, and protect storage devices: both local and networked Automate system security 24/7 by writing and scheduling scripts Maintain network services, encrypt network connections, and secure network-accessible processes Examine which processes are running—and which may represent a threat Use system logs to pinpoint potential vulnerabilities Keep Linux up-to-date with Red Hat or Debian software management tools Modify boot processes to harden security Master

advanced techniques for gathering system information

This revised and updated Second Edition presents a practical introduction to operating systems and illustrates these principles through a hands-on approach using accompanying simulation models developed in Java and C++. This text is appropriate for upper-level undergraduate courses in computer science. Case studies throughout the text feature the implementation of Java and C++ simulation models, giving students a thorough look at both the theoretical and the practical concepts discussed in modern OS courses. This pedagogical approach is designed to present a clearer, more practical look at OS concepts, techniques, and methods without sacrificing the theoretical rigor that is necessary at this level. It is an ideal choice for those interested in gaining comprehensive, hands-on experience using the modern techniques and methods necessary for working with these complex systems. Every new printed copy is accompanied with a CD-ROM containing simulations (eBook version does not include CD-ROM). New material added to the Second Edition: - Chapter 11 (Security) has been revised to include the most up-to-date information - Chapter 12 (Firewalls and Network Security) has been updated to include material on middleware that allows applications on separate machines to communicate (e.g. RMI, COM+, and Object Broker) - Includes a new chapter dedicated to Virtual Machines - Provides introductions to various types of scams - Updated to include information on Windows 7 and Mac OS X throughout the text - Contains new material on basic hardware architecture that operating systems depend on - Includes new material on handling multi-core CPUs Instructor Resources: -Answers to the end of chapter questions -PowerPoint Lecture Outlines

"The Second Edition of Security Strategies in Linux Platforms and Applications opens with a discussion of risks, threats, and vulnerabilities. Part 2 discusses how to take advantage of the layers of security and the modules associated with AppArmor and SELinux. Part 3 looks at the use of open source and proprietary tools when building a layered security strategy"--

When Practical Unix Security was first published more than a decade ago, it became an instant classic. Crammed with information about host security, it saved many a Unix system administrator from disaster. The second edition added much-needed Internet security coverage and doubled the size of the original volume. The third edition is a comprehensive update of this very popular book - a companion for the Unix/Linux system administrator who needs to secure his or her organization's system, networks, and web presence in an increasingly hostile world. Focusing on the four most popular Unix variants today--Solaris, Mac OS X, Linux, and FreeBSD--this book contains new information on PAM (Pluggable Authentication Modules), LDAP, SMB/Samba, anti-theft technologies, embedded systems, wireless and laptop issues, forensics, intrusion detection, chroot jails, telephone scanners and firewalls, virtual and cryptographic filesystems, WebNFS, kernel security levels, outsourcing, legal issues, new Internet protocols and cryptographic algorithms, and much more. Practical Unix &

Internet Security consists of six parts: Computer security basics: introduction to security problems and solutions, Unix history and lineage, and the importance of security policies as a basic element of system security. Security building blocks: fundamentals of Unix passwords, users, groups, the Unix filesystem, cryptography, physical security, and personnel security. Network security: a detailed look at modem and dialup security, TCP/IP, securing individual network services, Sun's RPC, various host and network authentication systems (e.g., NIS, NIS+, and Kerberos), NFS and other filesystems, and the importance of secure programming. Secure operations: keeping up to date in today's changing security world, backups, defending against attacks, performing integrity management, and auditing. Handling security incidents: discovering a break-in, dealing with programmed threats and denial of service attacks, and legal aspects of computer security. Appendixes: a comprehensive security checklist and a detailed bibliography of paper and electronic references for further reading and research. Packed with 1000 pages of helpful text, scripts, checklists, tips, and warnings, this third edition remains the definitive reference for Unix administrators and anyone who cares about protecting their systems and data from today's threats. Offers a readable, practical introduction and step-by-step procedural manual for the installation, configuration, and use of SELinux, a kernel module and set of Linux programs developed by the National Security Agency to help protect computers running on Linux. Original. (All users)

Router Security Strategies: Securing IP Network Traffic Planes provides a comprehensive approach to understand and implement IP traffic plane separation and protection on IP routers. This book details the distinct traffic planes of IP networks and the advanced techniques necessary to operationally secure them. This includes the data, control, management, and services planes that provide the infrastructure for IP networking. The first section provides a brief overview of the essential components of the Internet Protocol and IP networking. At the end of this section, you will understand the fundamental principles of defense in depth and breadth security as applied to IP traffic planes. Techniques to secure the IP data plane, IP control plane, IP management plane, and IP services plane are covered in detail in the second section. The final section provides case studies from both the enterprise network and the service provider network perspectives. In this way, the individual IP traffic plane security techniques reviewed in the second section of the book are brought together to help you create an integrated, comprehensive defense in depth and breadth security architecture. "Understanding and securing IP traffic planes are critical to the overall security posture of the IP infrastructure. The techniques detailed in this book provide protection and instrumentation enabling operators to understand and defend against attacks. As the vulnerability economy continues to mature, it is critical for both vendors and network providers to collaboratively deliver these protections to the IP infrastructure." –Russell Smoak, Director, Technical Services, Security Intelligence Engineering, Cisco Gregg Schudel,

CCIE® No. 9591, joined Cisco in 2000 as a consulting system engineer supporting the U.S. service provider organization. Gregg focuses on IP core network security architectures and technology for interexchange carriers and web services providers. David J. Smith, CCIE No. 1986, joined Cisco in 1995 and is a consulting system engineer supporting the service provider organization. David focuses on IP core and edge architectures including IP routing, MPLS technologies, QoS, infrastructure security, and network telemetry. Understand the operation of IP networks and routers Learn about the many threat models facing IP networks, Layer 2 Ethernet switching environments, and IPsec and MPLS VPN services Learn how to segment and protect each IP traffic plane by applying defense in depth and breadth principles Use security techniques such as ACLs, rate limiting, IP Options filtering, uRPF, QoS, RTBH, QPPB, and many others to protect the data plane of IP and switched Ethernet networks Secure the IP control plane with rACL, CoPP, GTSM, MD5, BGP and ICMP techniques and Layer 2 switched Ethernet-specific techniques Protect the IP management plane with password management, SNMP, SSH, NTP, AAA, as well as other VPN management, out-of-band management, and remote access management techniques Secure the IP services plane using recoloring, IP fragmentation control, MPLS label control, and other traffic classification and process control techniques This security book is part of the Cisco Press® Networking Technology Series. Security titles from Cisco Press help networking professionals secure critical data and resources, prevent and mitigate network attacks, and build end-to-end self-defending networks.

With more than 600 security tools in its arsenal, the Kali Linux distribution can be overwhelming. Experienced and aspiring security professionals alike may find it challenging to select the most appropriate tool for conducting a given test. This practical book covers Kali's expansive security capabilities and helps you identify the tools you need to conduct a wide range of security tests and penetration tests. You'll also explore the vulnerabilities that make those tests necessary. Author Ric Messier takes you through the foundations of Kali Linux and explains methods for conducting tests on networks, web applications, wireless security, password vulnerability, and more. You'll discover different techniques for extending Kali tools and creating your own toolset. Learn tools for stress testing network stacks and applications Perform network reconnaissance to determine what's available to attackers Execute penetration tests using automated exploit tools such as Metasploit Use cracking tools to see if passwords meet complexity requirements Test wireless capabilities by injecting frames and cracking passwords Assess web application vulnerabilities with automated or proxy-based tools Create advanced attack techniques by extending Kali tools or developing your own Use Kali Linux to generate reports once testing is complete The open source nature of the platform has not only established a new direction for the industry, but enables a developer or forensic analyst to understand the device at the most fundamental level. Android Forensics covers an open source

mobile device platform based on the Linux 2.6 kernel and managed by the Open Handset Alliance. The Android platform is a major source of digital forensic investigation and analysis. This book provides a thorough review of the Android platform including supported hardware devices, the structure of the Android development project and implementation of core services (wireless communication, data storage and other low-level functions). Finally, it will focus on teaching readers how to apply actual forensic techniques to recover data. Ability to forensically acquire Android devices using the techniques outlined in the book Detailed information about Android applications needed for forensics investigations Important information about SQLite, a file based structured data storage relevant for both Android and many other platforms.

An informative handbook for network administrators and professionals who use Linux offers practical guidelines on how to test, hack, and find security holes and secure them, explaining how to assess one's system, shut down unnecessary services and access, install filters and firewalls, eliminate unnecessary software, enhance authentication and user identity protocols, monitor network systems, and other important topics. Original. (Intermediate)

SELinux: Bring World-Class Security to Any Linux Environment! SELinux offers Linux/UNIX integrators, administrators, and developers a state-of-the-art platform for building and maintaining highly secure solutions. Now that SELinux is included in the Linux 2.6 kernel—and delivered by default in Fedora Core, Red Hat Enterprise Linux, and other major distributions—it's easier than ever to take advantage of its benefits. SELinux by Example is the first complete, hands-on guide to using SELinux in production environments. Authored by three leading SELinux researchers and developers, it illuminates every facet of working with SELinux, from its architecture and security object model to its policy language. The book thoroughly explains SELinux sample policies—including the powerful new Reference Policy—showing how to quickly adapt them to your unique environment. It also contains a comprehensive SELinux policy language reference and covers exciting new features in Fedora Core 5 and the upcoming Red Hat Enterprise Linux version 5.

- Thoroughly understand SELinux's access control and security mechanisms
- Use SELinux to construct secure systems from the ground up
- Gain fine-grained control over kernel resources
- Write policy statements for type enforcement, roles, users, and constraints
- Use optional multilevel security to enforce information classification and manage users with diverse clearances
- Create conditional policies that can be changed on-the-fly
- Define, manage, and maintain SELinux security policies
- Develop and write new SELinux security policy modules
- Leverage emerging SELinux technologies to gain even greater flexibility
- Effectively administer any SELinux system

Network security is not simply about building impenetrable walls—determined attackers will eventually overcome traditional defenses. The most effective computer security strategies integrate network security monitoring (NSM): the

collection and analysis of data to help you detect and respond to intrusions. In *The Practice of Network Security Monitoring*, Mandiant CSO Richard Bejtlich shows you how to use NSM to add a robust layer of protection around your networks—no prior experience required. To help you avoid costly and inflexible solutions, he teaches you how to deploy, build, and run an NSM operation using open source software and vendor-neutral tools. You'll learn how to:

- Determine where to deploy NSM platforms, and size them for the monitored networks
- Deploy stand-alone or distributed NSM installations
- Use command line and graphical packet analysis tools, and NSM consoles
- Interpret network evidence from server-side and client-side intrusions
- Integrate threat intelligence into NSM software to identify sophisticated adversaries

There's no foolproof way to keep attackers out of your network. But when they get in, you'll be prepared. *The Practice of Network Security Monitoring* will show you how to build a security net to detect, contain, and control them. Attacks are inevitable, but losing sensitive data shouldn't be.

Details all the Linux system holes, attack methods, and hacker's tools that hackers have had years to study, explore, and improve upon, helping Linux administrators identify and plug security holes on their systems. Original. (Intermediate/Advanced).

To thoroughly understand what makes Linux tick and why it's so efficient, you need to delve deep into the heart of the operating system--into the Linux kernel itself. The kernel is Linux--in the case of the Linux operating system, it's the only bit of software to which the term "Linux" applies. The kernel handles all the requests or completed I/O operations and determines which programs will share its processing time, and in what order. Responsible for the sophisticated memory management of the whole system, the Linux kernel is the force behind the legendary Linux efficiency. The new edition of *Understanding the Linux Kernel* takes you on a guided tour through the most significant data structures, many algorithms, and programming tricks used in the kernel. Probing beyond the superficial features, the authors offer valuable insights to people who want to know how things really work inside their machine. Relevant segments of code are dissected and discussed line by line. The book covers more than just the functioning of the code, it explains the theoretical underpinnings for why Linux does things the way it does. The new edition of the book has been updated to cover version 2.4 of the kernel, which is quite different from version 2.2: the virtual memory system is entirely new, support for multiprocessor systems is improved, and whole new classes of hardware devices have been added. The authors explore each new feature in detail. Other topics in the book include: Memory management including file buffering, process swapping, and Direct memory Access (DMA) The Virtual Filesystem and the Second Extended Filesystem Process creation and scheduling Signals, interrupts, and the essential interfaces to device drivers Timing Synchronization in the kernel Interprocess Communication (IPC) Program execution *Understanding the Linux Kernel*,

Read Book Security Strategies In Linux Platforms And Applications Jones Bartlett Learning Information Systems Security Assurance

Second Edition will acquaint you with all the inner workings of Linux, but is more than just an academic exercise. You'll learn what conditions bring out Linux's best performance, and you'll see how it meets the challenge of providing good system response during process scheduling, file access, and memory management in a wide variety of environments. If knowledge is power, then this book will help you make the most of your Linux system.

Can a system be considered truly reliable if it isn't fundamentally secure? Or can it be considered secure if it's unreliable? Security is crucial to the design and operation of scalable systems in production, as it plays an important part in product quality, performance, and availability. In this book, experts from Google share best practices to help your organization design scalable and reliable systems that are fundamentally secure. Two previous O'Reilly books from Google—Site Reliability Engineering and The Site Reliability Workbook—demonstrated how and why a commitment to the entire service lifecycle enables organizations to successfully build, deploy, monitor, and maintain software systems. In this latest guide, the authors offer insights into system design, implementation, and maintenance from practitioners who specialize in security and reliability. They also discuss how building and adopting their recommended best practices requires a culture that's supportive of such change. You'll learn about secure and reliable systems through:

- Design strategies
- Recommendations for coding, testing, and debugging practices
- Strategies to prepare for, respond to, and recover from incidents
- Cultural best practices that help teams across your organization collaborate effectively
- Provides advice on ways to ensure network security, covering such topics as DNS, Apache web server, OpenLDAP, email encryption, Cyrus IMAP service, and FTP server.

PART OF THE NEW JONES & BARTLETT LEARNING INFORMATION SYSTEMS SECURITY & ASSURANCE SERIES! Security Strategies in Linux Platforms and Applications covers every major aspect of security on a Linux system. Written by an industry expert, this book is divided into three natural parts to illustrate key concepts in the field. It opens with a discussion on the risks, threats, and vulnerabilities associated with Linux as an operating system using examples from Red Hat Enterprise Linux and Ubuntu. Part 2 discusses how to take advantage of the layers of security available to Linux--user and group options, filesystems, and security options for important services, as well as the security modules associated with AppArmor and SELinux. The book closes with a look at the use of both open source and proprietary tools when building a layered security strategy for Linux operating system environments. Using real-world examples and exercises, this useful resource incorporates hands-on activities to walk students through the fundamentals of security strategies related to the Linux system.

Discover and learn one of the most reliable and easy-to-use Operating Systems around! Do you want an excellent Operating System and be able to use it for

FREE? Come on, you're close on the right path of discovering and experiencing it! If you are in need of a fast, reliable, secured, flexible, easy to use and understand, and most importantly, it is a compatible software to all devices; here it is, the Linux Operating System. Linux is one of the most reliable Operating System (OS), a fast way to use different applications, and it's FREE to use and download. That makes this Operating System stand out with the others. It is just ONE CLICK away and you'll enjoy the perks of having this OS in your own computers or devices. More than anything, Linux can be used for a variety of applications. Whether you're opting to create a better system for business, or just want to be more creative and play around with things, Linux can help you do a great job. If you're too curious and eager enough to know more about this Operating System (OS) and its process, this book will help you understand it better. The "Linux Mastery - The Ultimate Linux Operating System and Command Line Mastery Guide" book gives you all the information that you want to know about this "one of a kind" Operating System. Moreover, in this book you will learn the following: * What is Linux? * Why Linux - The Benefits of Linux * Choosing a Distribution * Preparing to Install Linux * Installing Linux * Using Linux for Work and Play * Getting to Know Commands * Managing Files and Directories * Administration and Security. Furthermore, this book contains proven steps and strategies on how to make use of Linux, whether for work or play, understand the commands that you have to use, choose distributions, and understand exactly why Linux matters - and more. So what are you waiting for? Experience and explore the Linux Operating System

[Copyright: 0907ed8f8270a54deee8a3d83c17b662](https://www.amazon.com/dp/0907ed8f8270a54deee8a3d83c17b662)