

Linux Server Hacks Volume Two Tips Tools For Connecting Monitoring And Troubleshooting V 2

Beginning Ethical Hacking with PythonBSD HacksKali Linux 2: Windows Penetration TestingLinux Basics for HackersMastering Linux Security and HardeningNetwork Security HacksPodcasting HacksHackingHacking For DummiesCoding FreedomUbuntuLinux Server SecurityLinux Server Hacks100 neue Linux-Server HacksHacking with KaliLinux Server HacksHackingLinux Server Hacks Volume li: Tips & Tools For Connecting, Monitoring, And TroubleshootingUbuntu HacksWireless HacksiPhone HacksLinux Hardening in Hostile NetworksLinux Server Hacks, Volume TwoHands on HackingLinux Server SecurityThe Linux Command LineLinux Multimedia HacksKali Linux RevealedMaximum Linux SecurityHacking-The art Of ExploitationHackers BewareLearning Kali LinuxLinux Server HacksHack Proofing ColdFusionLinux Basics for HackersBeginning Ethical Hacking with Kali LinuxSQL HacksDevOps TroubleshootingKali Linux - An Ethical Hacker's CookbookWireless Hacks

Beginning Ethical Hacking with Python

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

BSD Hacks

Introduces more than one hundred effective ways to ensure security in a Linux, UNIX, or Windows network, covering both TCP/IP-based services and host-based security techniques, with examples of applied encryption, intrusion detections, and logging.

Kali Linux 2: Windows Penetration Testing

Provides advice and tools to help Linux system administrators solve problems, offering hacks devoted to concerns such as improving efficiency, tracking revisions

Download Ebook Linux Server Hacks Volume Two Tips Tools For Connecting Monitoring And Troubleshooting V 2

to system files, and tracking system performance.

Linux Basics for Hackers

Explains how to create a professional-quality Internet radio broadcast, with sections on selecting the right software, creating quality sound, building a show, distributing a podcast, audio editing, videocasting, and more. Original. (Intermediate)

Mastering Linux Security and Hardening

Linux Server Security has been written for Sysadmins, DevOps engineers, developers and other technical professionals that wish to improve their hands-on knowledge of securing what is now the most popular Operating System on the planet. This detailed book walks steadily through challenging scenarios so that the reader may increase their knowledge of a number of diverse security areas which a technical professional faces. The reader is already familiar with Linux as a bedrock of stability but sometimes frustrated with certain software packages and the way that they integrate with the Operating System and indeed other packages. Looking closely at a considered selection of security topics empowers the reader to continue their learning and make full use of Linux's rocksteady foundation. In addition to each of the varied subjects covered such as sophisticated attacks, penetration testing, launching attacks and making a server invisible the book is brimming with invaluable insights gleaned from hard-won, professional experience. Applicable to almost all of the popular Linux flavours, such as Debian, Red Hat, Ubuntu, Linux Mint and CentOS, Linux Server Security can also be used to reference other Unix-type systems with little modification. The reader will improve their practical knowhow and background knowledge in order to increase their ability to troubleshoot and ultimately solve the daily security challenges encountered by Sysadmins and DevOps engineers. Whether the aim is to further a career or bring more enjoyment to a hobby the powerful, newfound knowledge gleaned from this book will help the reader add to their technical arsenal.

Network Security Hacks

A competent system administrator knows that a Linux server is a high performance system for routing large amounts of information through a network connection. Setting up and maintaining a Linux server requires understanding not only the hardware, but the ins and outs of the Linux operating system along with its supporting cast of utilities as well as layers of applications software. There's basic documentation online but there's a lot beyond the basics you have to know, and this only comes from people with hands-on, real-world experience. This kind of "know how" is what we sought to capture in Linux Server Hacks. Linux Server Hacks is a collection of 100 industrial-strength hacks, providing tips and tools that solve practical problems for Linux system administrators. Every hack can be read in just a few minutes but will save hours of searching for the right answer. Some of the hacks are subtle, many of them are non-obvious, and all of them demonstrate the power and flexibility of a Linux system. You'll find hacks devoted to tuning the Linux kernel to make your system run more efficiently, as well as using CVS or RCS

Download Ebook Linux Server Hacks Volume Two Tips Tools For Connecting Monitoring And Troubleshooting V 2

to track the revision to system files. You'll learn alternative ways to do backups, how to use system monitoring tools to track system performance and a variety of secure networking solutions. Linux Server Hacks also helps you manage large-scale Web installations running Apache, MySQL, and other open source tools that are typically part of a Linux system. O'Reilly's new Hacks Series proudly reclaims the term "hacking" for the good guys. Hackers use their ingenuity to solve interesting problems. Rob Flickenger is an experienced system administrator, having managed the systems for O'Reilly Network for several years. (He's also into community wireless networking and he's written a book on that subject for O'Reilly.) Rob has also collected the best ideas and tools from a number of other highly skilled contributors. Written for users who already understand the basics, Linux Server Hacks is built upon the expertise of people who really know what they're doing.

Podcasting Hacks

Linux Server Hacks 2 covers a wide variety of topics like replication, emulation, authentication, print management, and file sharing. Essential security and lockdown instructions are included for SELinux and firewall users. Coverage of advanced system administration hacks are included for topics such as request tracking, web mail, and shared calendars. While it's an ideal follow-up to Linux Server Hacks, this book is a valuable asset all on its own.

Hacking

A new edition of the bestselling guide--now updated to cover the latest hacks and how to prevent them! It's bad enough when a hack occurs--stealing identities, bank accounts, and personal information. But when the hack could have been prevented by taking basic security measures--like the ones described in this book--somehow that makes a bad situation even worse. This beginner guide to hacking examines some of the best security measures that exist and has been updated to cover the latest hacks for Windows 7 and the newest version of Linux. Offering increased coverage of Web application hacks, database hacks, VoIP hacks, and mobile computing hacks, this guide addresses a wide range of vulnerabilities and how to identify and prevent them. Plus, you'll examine why ethical hacking is oftentimes the only way to find security flaws, which can then prevent any future malicious attacks. Explores the malicious hackers's mindset so that you can counteract or avoid attacks completely Covers developing strategies for reporting vulnerabilities, managing security changes, and putting anti-hacking policies and procedures in place Completely updated to examine the latest hacks to Windows 7 and the newest version of Linux Explains ethical hacking and why it is essential Hacking For Dummies, 3rd Edition shows you how to put all the necessary security measures in place so that you avoid becoming a victim of malicious hacking.

Hacking For Dummies

Who are computer hackers? What is free software? And what does the emergence of a community dedicated to the production of free and open source software--and to hacking as a technical, aesthetic, and moral project--reveal about the values of contemporary liberalism? Exploring the rise and political significance of the free

Download Ebook Linux Server Hacks Volume Two Tips Tools For Connecting Monitoring And Troubleshooting V 2

and open source software (F/OSS) movement in the United States and Europe, Coding Freedom details the ethics behind hackers' devotion to F/OSS, the social codes that guide its production, and the political struggles through which hackers question the scope and direction of copyright and patent law. In telling the story of the F/OSS movement, the book unfolds a broader narrative involving computing, the politics of access, and intellectual property. E. Gabriella Coleman tracks the ways in which hackers collaborate and examines passionate manifestos, hacker humor, free software project governance, and festive hacker conferences. Looking at the ways that hackers sustain their productive freedom, Coleman shows that these activists, driven by a commitment to their work, reformulate key ideals including free speech, transparency, and meritocracy, and refuse restrictive intellectual protections. Coleman demonstrates how hacking, so often marginalized or misunderstood, sheds light on the continuing relevance of liberalism in online collaboration.

Coding Freedom

A comprehensive guide to mastering the art of preventing your Linux system from getting compromised. Key Features Leverage this guide to confidently deliver a system that reduces the risk of being hacked Perform a number of advanced Linux security techniques such as network service detection, user authentication, controlling special permissions, encrypting file systems, and much more Master the art of securing a Linux environment with this end-to-end practical guide Book Description This book has extensive coverage of techniques that will help prevent attackers from breaching your system, by building a much more secure Linux environment. You will learn various security techniques such as SSH hardening, network service detection, setting up firewalls, encrypting file systems, protecting user accounts, authentication processes, and so on. Moving forward, you will also develop hands-on skills with advanced Linux permissions, access control, special modes, and more. Lastly, this book will also cover best practices and troubleshooting techniques to get your work done efficiently. By the end of this book, you will be confident in delivering a system that will be much harder to compromise. What you will learn Use various techniques to prevent intruders from accessing sensitive data Prevent intruders from planting malware, and detect whether malware has been planted Prevent insiders from accessing data that they aren't authorized to access Do quick checks to see whether a computer is running network services that it doesn't need to run Learn security techniques that are common to all Linux distros, and some that are distro-specific Who this book is for If you are a systems administrator or a network engineer interested in making your Linux environment more secure, then this book is for you. Security consultants wanting to enhance their Linux security skills will also benefit from this book. Prior knowledge of Linux is mandatory.

Ubuntu

Many aspiring hackers are unfamiliar with Linux, having learned computer basics in a Windows or Mac environment. This can pose the single most important obstacle to mastering the skills to becoming a better hacker; while hacking can be done with Windows or OS X, nearly all hacking tools are developed specifically for Linux. Linux Basics for Hackers aims to provide you with a foundation of Linux skills that

Download Ebook Linux Server Hacks Volume Two Tips Tools For Connecting Monitoring And Troubleshooting V 2

every hacker needs. As you progress, you'll have access to numerous real-world examples and hands-on exercises to apply your new knowledge and bring yourself up to speed.

Linux Server Security

Explains how and why hackers break into computers, steal information, and deny services to machines' legitimate users, and discusses strategies and tools used by hackers and how to defend against them.

Linux Server Hacks

Implement Industrial-Strength Security on Any Linux Server In an age of mass surveillance, when advanced cyberwarfare weapons rapidly migrate into every hacker's toolkit, you can't rely on outdated security methods—especially if you're responsible for Internet-facing services. In *Linux® Hardening in Hostile Networks*, Kyle Rankin helps you to implement modern safeguards that provide maximum impact with minimum effort and to strip away old techniques that are no longer worth your time. Rankin provides clear, concise guidance on modern workstation, server, and network hardening, and explains how to harden specific services, such as web servers, email, DNS, and databases. Along the way, he demystifies technologies once viewed as too complex or mysterious but now essential to mainstream Linux security. He also includes a full chapter on effective incident response that both DevOps and SecOps can use to write their own incident response plan. Each chapter begins with techniques any sysadmin can use quickly to protect against entry-level hackers and presents intermediate and advanced techniques to safeguard against sophisticated and knowledgeable attackers, perhaps even state actors. Throughout, you learn what each technique does, how it works, what it does and doesn't protect against, and whether it would be useful in your environment. Apply core security techniques including 2FA and strong passwords Protect admin workstations via lock screens, disk encryption, BIOS passwords, and other methods Use the security-focused Tails distribution as a quick path to a hardened workstation Compartmentalize workstation tasks into VMs with varying levels of trust Harden servers with SSH, use apparmor and sudo to limit the damage attackers can do, and set up remote syslog servers to track their actions Establish secure VPNs with OpenVPN, and leverage SSH to tunnel traffic when VPNs can't be used Configure a software load balancer to terminate SSL/TLS connections and initiate new ones downstream Set up standalone Tor services and hidden Tor services and relays Secure Apache and Nginx web servers, and take full advantage of HTTPS Perform advanced web server hardening with HTTPS forward secrecy and ModSecurity web application firewalls Strengthen email security with SMTP relay authentication, SMTPS, SPF records, DKIM, and DMARC Harden DNS servers, deter their use in DDoS attacks, and fully implement DNSSEC Systematically protect databases via network access control, TLS traffic encryption, and encrypted data storage Respond to a compromised server, collect evidence, and prevent future attacks Register your product at informit.com/register for convenient access to downloads, updates, and corrections as they become available.

100 neue Linux-Server Hacks

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 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?

Hacking with Kali

"If you're a developer trying to figure out why your application is not responding at 3 am, you need this book! This is now my go-to book when diagnosing production issues. It has saved me hours in troubleshooting complicated operations problems." -Trotter Cashion, cofounder, Mashion DevOps can help developers, QAs, and admins work together to solve Linux server problems far more rapidly, significantly improving IT performance, availability, and efficiency. To gain these benefits, however, team members need common troubleshooting skills and practices. In DevOps Troubleshooting: Linux Server Best Practices, award-winning Linux expert Kyle Rankin brings together all the standardized, repeatable techniques your team needs to stop finger-pointing, collaborate effectively, and quickly solve virtually any Linux server problem. Rankin walks you through using DevOps techniques to troubleshoot everything from boot failures and corrupt disks to lost email and downed websites. You'll master indispensable skills for diagnosing high-load systems and network problems in production environments. Rankin shows how to Master DevOps' approach to troubleshooting and proven Linux server problem-solving principles Diagnose slow servers and applications by identifying CPU, RAM, and Disk I/O bottlenecks Understand healthy boots, so you can identify failure points and fix them Solve full or corrupt disk issues that prevent disk writes Track down the sources of network problems Troubleshoot DNS, email, and other network services Isolate and diagnose Apache and Nginx Web server failures and slowdowns Solve problems with MySQL and Postgres database servers and queries Identify hardware failures—even notoriously elusive intermittent failures

Linux Server Hacks

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).

Hacking

Provides tips and techniques on wireless networking, covering a variety of topics, including wireless standards, Bluetooth, hardware, antennas, and wireless security.

Linux Server Hacks Volume II: Tips & Tools For Connecting, Monitoring, And Troubleshooting

A guide to getting the most out of the SQL language covers such topics as sending SQL commands to a database, using advanced techniques, solving puzzles, performing searches, and managing users.

Ubuntu Hacks

This book is a guide on how to use Kali Linux for penetration testing. It begins by guiding you on how to use the "Sqlmap" tool to perform an SQL injection. This will help you seal any loopholes in your databases. The book then guides you on how to use a tool named "Fluxion" so as to hack networks which are protected by WPA/WPA2. Brute forcing has been used for carrying out this kind of attack. You will also learn how to check or know the location for a particular IP address in the world. You will learn how to get details about this location in terms of longitude, country, and other parameters. The process of hiding or spoofing MAC addresses for your devices is very important for penetration testing. This book guides you on how to spoof the MAC address of your devices. After developing a website or before you can hack a website, it is good for you to scan it and identify any loopholes or vulnerabilities within it. You can then go ahead and exploit these vulnerabilities, or seal them to prevent a disaster. This book guides you on how to scan a website and identify any vulnerability within it. You are guided on how to hack Android phones by the use of Kali Linux. HTTP servers usually have an open FTP port. This book guides you on how to use this port and gain access to the server. You will also know how to carry out a mass mailer attack, as well as password cracking in Kali Linux. The following topics are discussed in this book: - Sqlmap for Website Hacking - How to Hack WPA/WPA2 without Brute Force - Checking for IP Address Location - MAC Address Spoofing - Scanning a Website for Vulnerability - Hacking Android Phones with Kali Linux -Hacking FTP Server in Kali Linux - Creating a Persistent Backdoor in Android - Mass Mailer Attack - Password Cracking

Wireless Hacks

Ubuntu Linux--the most popular Linux distribution on the planet--preserves the spirit embodied in the ancient African word ubuntu, which means both "humanity

Download Ebook Linux Server Hacks Volume Two Tips Tools For Connecting Monitoring And Troubleshooting V 2

to others" and "I am what I am because of who we all are." Ubuntu won the Linux Journal Reader's Choice Award for best Linux distribution and is consistently the top-ranked Linux variant on DistroWatch.com. The reason this distribution is so widely popular is that Ubuntu is designed to be useful, usable, customizable, and always available for free worldwide. Ubuntu Hacks is your one-stop source for all of the community knowledge you need to get the most out of Ubuntu: a collection of 100 tips and tools to help new and experienced Linux users install, configure, and customize Ubuntu. With this set of hacks, you can get Ubuntu Linux working exactly the way you need it to. Learn how to: Install and test-drive Ubuntu Linux. Keep your system running smoothly Turn Ubuntu into a multimedia powerhouse: rip and burn discs, watch videos, listen to music, and more Take Ubuntu on the road with Wi-Fi wireless networking, Bluetooth, etc. Hook up multiple displays and enable your video card's 3-D acceleration Run Ubuntu with virtualization technology such as Xen and VMware Tighten your system's security Set up an Ubuntu-powered server Ubuntu Hacks will not only show you how to get everything working just right, you will also have a great time doing it as you explore the powerful features lurking within Ubuntu. "Put in a nutshell, this book is a collection of around 100 tips and tricks which the authors choose to call hacks, which explain how to accomplish various tasks in Ubuntu Linux. The so called hacks range from down right ordinary to the other end of the spectrum of doing specialised things More over, each and every tip in this book has been tested by the authors on the latest version of Ubuntu (Dapper Drake) and is guaranteed to work. In writing this book, it is clear that the authors have put in a lot of hard work in covering all facets of configuring this popular Linux distribution which makes this book a worth while buy." -- Ravi Kumar, Slashdot.org

iPhone Hacks

You've experienced the shiny, point-and-click surface of your Linux computer—now dive below and explore its depths with the power of the command line. The Linux Command Line takes you from your very first terminal keystrokes to writing full programs in Bash, the most popular Linux shell. Along the way you'll learn the timeless skills handed down by generations of gray-bearded, mouse-shunning gurus: file navigation, environment configuration, command chaining, pattern matching with regular expressions, and more. In addition to that practical knowledge, author William Shotts reveals the philosophy behind these tools and the rich heritage that your desktop Linux machine has inherited from Unix supercomputers of yore. As you make your way through the book's short, easily-digestible chapters, you'll learn how to: * Create and delete files, directories, and symlinks * Administer your system, including networking, package installation, and process management * Use standard input and output, redirection, and pipelines * Edit files with Vi, the world's most popular text editor * Write shell scripts to automate common or boring tasks * Slice and dice text files with cut, paste, grep, patch, and sed Once you overcome your initial "shell shock," you'll find that the command line is a natural and expressive way to communicate with your computer. Just don't be surprised if your mouse starts to gather dust. A featured resource in the Linux Foundation's "Evolution of a SysAdmin"

Linux Hardening in Hostile Networks

Download Ebook Linux Server Hacks Volume Two Tips Tools For Connecting Monitoring And Troubleshooting V 2

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.

Linux Server Hacks, Volume Two

With iPhone Hacks, you can make your iPhone do all you'd expect of a mobile smartphone -- and more. Learn tips and techniques to unleash little-known features, find and create innovative applications for both the iPhone and iPod touch, and unshackle these devices to run everything from network utilities to video game emulators. This book will teach you how to: Import your entire movie collection, sync with multiple computers, and save YouTube videos Remotely access your home network, audio, and video, and even control your desktop Develop native applications for the iPhone and iPod touch on Linux, Windows, or Mac Check email, receive MMS messages, use IRC, and record full-motion video Run any application in the iPhone's background, and mirror its display on a TV Make your iPhone emulate old-school video game platforms, and play classic console and arcade games Integrate your iPhone with your car stereo Build your own electronic bridges to connect keyboards, serial devices, and more to your iPhone without "jailbreaking" iPhone Hacks explains how to set up your iPhone the way you want it, and helps you give it capabilities that will rival your desktop computer. This cunning little handbook is exactly what you need to make the most of your iPhone.

Hands on Hacking

Linux Server Security

Learn the basics of ethical hacking and gain insights into the logic, algorithms, and syntax of Python. This book will set you up with a foundation that will help you understand the advanced concepts of hacking in the future. Learn Ethical Hacking with Python 3 touches the core issues of cyber security: in the modern world of interconnected computers and the Internet, security is increasingly becoming one of the most important features of programming. Ethical hacking is closely related to Python. For this reason this book is organized in three parts. The first part deals with the basics of ethical hacking; the second part deals with Python 3; and the third part deals with more advanced features of ethical hacking. What You Will Learn Discover the legal constraints of ethical hacking Work with virtual machines and virtualization Develop skills in Python 3 See the importance of networking in ethical hacking Gain knowledge of the dark web, hidden Wikipedia, proxy chains, virtual private networks, MAC addresses, and more Who This Book Is For Beginners wanting to learn ethical hacking alongside a modular object oriented programming language.

The Linux Command Line

This text introduces the spirit and theory of hacking as well as the science behind it all; it also provides some core techniques and tricks of hacking so you can think like a hacker, write your own hacks or thwart potential system attacks.

Linux Multimedia Hacks

In the world of Unix operating systems, the various BSDs come with a long heritage of high-quality software without restrictions. Steeped in the venerable Unix traditions the immense power and flexibility of the BSDs are yours to hack. Of course, first you have to know what you have at hand and how to use it. Written by trainers, developers, hobbyists, and administrators, BSD Hacks collects 100 tips and tricks to fill your toolbox. Whether you're a new user, an administrator, or a power user looking for new ideas to take your knowledge to the next level, each hack will let you peek inside the mind of another Unix fan. Learn how to : Customize and install software exactly as you want it on one or dozens of machines ; Configure the command line the way you like it, to speed up common tasks and make difficult things easy ; Be a good network neighbor, even to other operating systems ; Make the most of the copious documentation or find (and document) answers when there's no documentation ; Allocate bandwidth by time, department, or use ; Secure your system with good passwords, intelligent firewall rules, proper logging, and a little foresight ; Plan for and recover from disaster, including catastrophic Internet loss and hardware failures ; Automate your backups, safely and securely. BSD Hacks is for anyone using FreeBSD, OpenBSD, NetBSD, Darwin (under or alongside Mac OS X), or anything else BSD-flavored. Whether you're new to BSD or an old hand-even seasoned Linux folk can Learn a lot from their cousins-you will reach new levels of understanding and have a lot of fun along the way.

Kali Linux Revealed

Download Ebook Linux Server Hacks Volume Two Tips Tools For Connecting Monitoring And Troubleshooting V 2

A fast, hands-on introduction to offensive hacking techniques Hands-On Hacking teaches readers to see through the eyes of their adversary and apply hacking techniques to better understand real-world risks to computer networks and data. Readers will benefit from the author's years of experience in the field hacking into computer networks and ultimately training others in the art of cyber-attacks. This book holds no punches and explains the tools, tactics and procedures used by ethical hackers and criminal crackers alike. We will take you on a journey through a hacker's perspective when focused on the computer infrastructure of a target company, exploring how to access the servers and data. Once the information gathering stage is complete, you'll look for flaws and their known exploits—including tools developed by real-world government financed state-actors.

- An introduction to the same hacking techniques that malicious hackers will use against an organization
- Written by infosec experts with proven history of publishing vulnerabilities and highlighting security flaws
- Based on the tried and tested material used to train hackers all over the world in the art of breaching networks
- Covers the fundamental basics of how computer networks are inherently vulnerable to attack, teaching the student how to apply hacking skills to uncover vulnerabilities

We cover topics of breaching a company from the external network perimeter, hacking internal enterprise systems and web application vulnerabilities. Delving into the basics of exploitation with real-world practical examples, you won't find any hypothetical academic only attacks here. From start to finish this book will take the student through the steps necessary to breach an organization to improve its security. Written by world-renowned cybersecurity experts and educators, Hands-On Hacking teaches entry-level professionals seeking to learn ethical hacking techniques. If you are looking to understand penetration testing and ethical hacking, this book takes you from basic methods to advanced techniques in a structured learning format.

Maximum Linux Security

Learn how to attack and defend the world's most popular web server platform Linux Server Security: Hack and Defend presents a detailed guide for experienced admins, aspiring hackers and other IT professionals seeking a more advanced understanding of Linux security. Written by a 20-year veteran of Linux server deployment this book provides the insight of experience along with highly practical instruction. The topics range from the theory of past, current, and future attacks, to the mitigation of a variety of online attacks, all the way to empowering you to perform numerous malicious attacks yourself (in the hope that you will learn how to defend against them). By increasing your understanding of a hacker's tools and mindset you're less likely to be confronted by the all-too-common reality faced by many admins these days: someone else has control of your systems. Master hacking tools and launch sophisticated attacks: perform SQL injections, deploy multiple server exploits and crack complex passwords. Defend systems and networks: make your servers invisible, be confident of your security with penetration testing and repel unwelcome attackers. Increase your background knowledge of attacks on systems and networks and improve all-important practical skills required to secure any Linux server. The techniques presented apply to almost all Linux distributions including the many Debian and Red Hat derivatives and some other Unix-type systems. Further your career with this intriguing, deeply insightful, must-have technical book. Diverse, broadly-applicable and hands-on

Download Ebook Linux Server Hacks Volume Two Tips Tools For Connecting Monitoring And Troubleshooting V 2

practical, Linux Server Security: Hack and Defend is an essential resource which will sit proudly on any techie's bookshelf.

Hacking- The art Of Exploitation

The only way to stop a hacker is to think like one! ColdFusion is a Web application development tool that allows programmers to quickly build robust applications using server-side markup language. It is incredibly popular and has both an established user base and a quickly growing number of new adoptions. It has become the development environment of choice for e-commerce sites and content sites where databases and transactions are the most vulnerable and where security is of the utmost importance. Several security concerns exist for ColdFusion due to its unique approach of designing pages using dynamic-page templates rather than static HTML documents. Because ColdFusion does not require that developers have expertise in Visual Basic, Java and C++; Web applications created using ColdFusion Markup language are vulnerable to a variety of security breaches. Hack Proofing ColdFusion 5.0 is the seventh edition in the popular Hack Proofing series and provides developers with step-by-step instructions for developing secure web applications. Teaches strategy and techniques: Using forensics-based analysis this book gives the reader insight to the mind of a hacker Interest in topic continues to grow: Network architects, engineers and administrators are scrambling for security books to help them protect their new networks and applications powered by ColdFusion Unrivalled Web-based support: Up-to-the minute links, white papers and analysis for two years at solutions@syngress.com

Hackers Beware

Learning Kali Linux

The authors bring readers more of the practical tips and tricks that made the first edition a runaway hit. Completely revised and updated, this version includes over 30 new hacks, major overhauls of over 30 more, and timely adjustments and touch-ups to dozens of other hacks.

Linux Server Hacks

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,

Download Ebook Linux Server Hacks Volume Two Tips Tools For Connecting Monitoring And Troubleshooting V 2

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

Hack Proofing ColdFusion

Provides instructions for a variety of multimedia projects that can be done with Linux, including creating DVDs and VCDs, streaming audio and video over the Internet, and building a MythTV digital media hub.

Linux Basics for Hackers

Kali Linux: a complete pentesting toolkit facilitating smooth backtracking for working hackers About This Book Conduct network testing, surveillance, pen testing and forensics on MS Windows using Kali Linux Footprint, monitor, and audit your network and investigate any ongoing infestations Customize Kali Linux with this professional guide so it becomes your pen testing toolkit Who This Book Is For If you are a working ethical hacker who is looking to expand the offensive skillset with a thorough understanding of Kali Linux, then this is the book for you. Prior knowledge about Linux operating systems and the BASH terminal emulator along with Windows desktop and command line would be highly beneficial. What You Will Learn Set up Kali Linux for pen testing Map and enumerate your Windows network Exploit several common Windows network vulnerabilities Attack and defeat password schemes on Windows Debug and reverse-engineer Windows programs Recover lost files, investigate successful hacks and discover hidden data in innocent-looking files Catch and hold admin rights on the network, and maintain backdoors on the network after your initial testing is done In Detail Microsoft Windows is one of the two most common OS and managing its security has spawned the discipline of IT security. Kali Linux is the premier platform for testing and maintaining Windows security. Kali is built on the Debian distribution of Linux and shares the legendary stability of that OS. This lets you focus on using the network penetration, password cracking, forensics tools and not the OS. This book has the most advanced tools and techniques to reproduce the methods used by sophisticated hackers to make you an expert in Kali Linux penetration testing. First, you are introduced to Kali's top ten tools and other useful reporting tools. Then, you will find your way around your target network and determine known vulnerabilities to be able to exploit a system remotely. Next, you will prove that the vulnerabilities you have found are real and exploitable. You will learn to use tools in seven categories of exploitation tools. Further, you perform web access exploits using tools like websploit and more. Security is only as strong as the weakest link in the chain. Passwords are often that weak link. Thus, you learn about password attacks that can be used in concert with other approaches to break into and own a network. Moreover, you come to terms with network sniffing, which helps you understand which users are using services you can exploit, and IP spoofing, which can be used to poison a system's DNS cache. Once you gain access to a machine or network, maintaining access is important. Thus, you not only learn penetrating in the machine you also learn Windows privilege's escalations. With easy to follow step-by-step instructions and support images, you will be able to quickly pen test your system and network. Style and approach This book is a hands-on guide for

Download Ebook Linux Server Hacks Volume Two Tips Tools For Connecting Monitoring And Troubleshooting V 2

Kali Linux pen testing. This book will provide all the practical knowledge needed to test your network's security using a proven hacker's methodology. The book uses easy-to-understand yet professional language for explaining concepts.

Beginning Ethical Hacking with Kali Linux

Whether you're a veteran or an absolute n00b, this is the best place to start with Kali Linux, the security professional's platform of choice, and a truly industrial-grade, and world-class operating system distribution-mature, secure, and enterprise-ready.

SQL Hacks

This Book, Hacking Practical Guide for Beginners is a comprehensive learning material for all inexperienced hackers. It is a short manual that describes the essentials of hacking. By reading this book, you'll arm yourself with modern hacking knowledge and techniques. However, do take note that this material is not limited to theoretical information. It also contains a myriad of practical tips, tricks, and strategies that you can use in hacking your targets. The first chapter of this book explains the basics of hacking and the different types of hackers. The second chapter has a detailed study plan for budding hackers. That study plan will help you improve your skills in a short period of time. The third chapter will teach you how to write your own codes using the Python programming language. The rest of the book contains detailed instructions on how you can become a skilled hacker and penetration tester. After reading this book, you'll learn how to: - Use the Kali Linux operating system - Set up a rigged WiFi hotspot - Write codes and programs using Python - Utilize the Metasploit framework in attacking your targets - Collect information using certain hacking tools - Conduct a penetration test - Protect your computer and network from other hackers - And a lot more Make sure you get your copy today!

DevOps Troubleshooting

Get started in white-hat ethical hacking using Kali Linux. This book starts off by giving you an overview of security trends, where you will learn the OSI security architecture. This will form the foundation for the rest of Beginning Ethical Hacking with Kali Linux. With the theory out of the way, you'll move on to an introduction to VirtualBox, networking, and common Linux commands, followed by the step-by-step procedure to build your own web server and acquire the skill to be anonymous. When you have finished the examples in the first part of your book, you will have all you need to carry out safe and ethical hacking experiments. After an introduction to Kali Linux, you will carry out your first penetration tests with Python and code raw binary packets for use in those tests. You will learn how to find secret directories on a target system, use a TCP client in Python, and scan ports using NMAP. Along the way you will discover effective ways to collect important information, track email, and use important tools such as DMITRY and Maltego, as well as take a look at the five phases of penetration testing. The coverage of vulnerability analysis includes sniffing and spoofing, why ARP poisoning is a threat, how Sniffjoke prevents poisoning, how to analyze protocols with Wireshark, and

Download Ebook Linux Server Hacks Volume Two Tips Tools For Connecting Monitoring And Troubleshooting V 2

using sniffing packets with Scapy. The next part of the book shows you detecting SQL injection vulnerabilities, using sqlmap, and applying brute force or password attacks. Besides learning these tools, you will see how to use OpenVas, Nikto, Vega, and Burp Suite. The book will explain the information assurance model and the hacking framework Metasploit, taking you through important commands, exploit and payload basics. Moving on to hashes and passwords you will learn password testing and hacking techniques with John the Ripper and Rainbow. You will then dive into classic and modern encryption techniques where you will learn the conventional cryptosystem. In the final chapter you will acquire the skill of exploiting remote Windows and Linux systems and you will learn how to own a target completely. What You Will Learn Master common Linux commands and networking techniques Build your own Kali web server and learn to be anonymous Carry out penetration testing using Python Detect sniffing attacks and SQL injection vulnerabilities Learn tools such as SniffJoke, Wireshark, Scapy, sqlmap, OpenVas, Nikto, and Burp Suite Use Metasploit with Kali Linux Exploit remote Windows and Linux systems Who This Book Is For Developers new to ethical hacking with a basic understanding of Linux programming.

Kali Linux - An Ethical Hacker's Cookbook

Today's system administrators deal with a vast number of situations, operating systems, software packages, and problems. Those who are in the know have kept their copy of Linux Server Hacks close at hand to ease their burden. And while this helps, it's not enough: any sys admin knows there are many more hacks, cool tips, and ways of solving problems than can fit in a single volume (one that mere mortals can lift, that is). Which is why we created Linux Server Hacks, Volume Two, a second collection of incredibly useful tips and tricks for finding and using dozens of open source tools you can apply to solve your sys admin problems. The power and flexibility of Linux and Open Source means that there is an astounding amount of great software out there waiting to be applied to your sys admin problems -- if only you knew about it and had enough information to get started. Hence, Linux Server Hacks, Volume Two. This handy reference offers 100 completely new server management tips and techniques designed to improve your productivity and sharpen your administrative skills. Each hack represents a clever way to accomplish a specific task, saving you countless hours of searching for the right answer. No more sifting through man pages, HOWTO websites, or source code comments -- the only resource you need is right here. And you don't have to be a system administrator with hundreds of boxes to get something useful from this book as many of the hacks apply equally well to a single system or a home network. Compiled by experts, these hacks not only give you the step-by-step instructions necessary to implement the software, but they also provide the context to truly enable you to learn the technology. Topics include: Authentication Remote GUI connectivity Storage management File sharing and synchronizing resources Security/lockdown instruction Log files and monitoring Troubleshooting System rescue, recovery, and repair Whether they help you recover lost data, collect information from distributed clients, or synchronize administrative environments, the solutions found in Linux Server Hacks, Volume Two will simplify your life as a system administrator.

Wireless Hacks

Download Ebook Linux Server Hacks Volume Two Tips Tools For Connecting Monitoring And Troubleshooting V 2

Download Ebook Linux Server Hacks Volume Two Tips Tools For
Connecting Monitoring And Troubleshooting V 2

[ROMANCE](#) [ACTION & ADVENTURE](#) [MYSTERY & THRILLER](#) [BIOGRAPHIES &
HISTORY](#) [CHILDREN'S](#) [YOUNG ADULT](#) [FANTASY](#) [HISTORICAL FICTION](#) [HORROR](#)
[LITERARY FICTION](#) [NON-FICTION](#) [SCIENCE FICTION](#)